

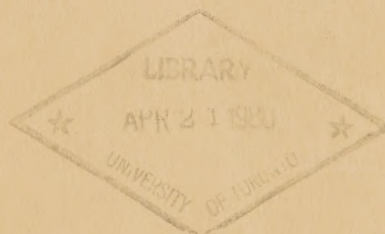
Digitized by the Internet Archive
in 2022 with funding from
University of Toronto

A2ΦN
AJ 811
-80P15



Commission on Freedom of Information and Individual Privacy

Privacy and Personal Data Protection



CA26N
AJ 811
-80P15



Commission

on

Freedom of Information

and

Individual Privacy

PRIVACY AND PERSONAL DATA PROTECTION

A Report on Personal Record-Keeping
by the Ministries and Agencies
of the Ontario Government

by Michael Brown,
Brenda Billingsley,
and Rebecca Shamai

Research Publication 15

Prepared for the
Commission on Freedom of Information
and Individual Privacy

March, 1980



(iii)

D. Carlton Williams, Ph.D.
Chairman
Dorothy J. Burgoyne, B.A.
G. H. U. Bayly, M.Sc.F.
Members

W. R. Poole, Q.C.
Counsel

J. D. McCamus, L.L.M.
Director of Research

Hon. J. C. McRuer, O.C.
Consultant

Doris E. Wagg
Registrar

Commission
on
Freedom of Information
and
Individual Privacy

416/598-0411

180 Dundas Street West
22nd Floor
Toronto Ontario
M5G 1Z8

FOREWORD

The Commission on Freedom of Information and Individual Privacy was established by the government of Ontario in March, 1977, to "study and report to the Attorney General of Ontario on ways and means to improve the public information policies and relevant legislation and procedures of the government of Ontario, and to examine:

1. Public information practices of other jurisdictions in order to consider possible changes which are compatible with the parliamentary traditions of the government of Ontario and complementary to the mechanisms that presently exist for the protection of the rights of individuals;
2. The individual's right of access and appeal in relation to the use of government information;
3. The categories of government information which should be treated as confidential in order to protect the public interest;
4. The effectiveness of present procedures for the dissemination of government information to the public;
5. The protection of individual privacy and the right of recourse in regard to the use of government records."

To the best of our knowledge it is the only Commission of its kind whose mandate embraces both freedom of information and individual privacy. The views of the public were embodied in the briefs submitted and in the series of hearings held in ten communities, and covering both Northern and Southern Ontario. In response to public demand, three sets of hearings, widely separated in time, were held in Toronto.

(iv)



The views of the scholars and experts in the field are to be found in the present series of research reports of which this is number 15. These, together with the briefs submitted, constitute the backbone of our findings: the stuff out of which our Report will be made. Many of these stand in their own right as documents of importance to this field of study; hence our decision to publish them immediately.

It is our confident expectation that they will be received by the interested public with the same interest and enthusiasm they generated in us. Many tackle problem areas never before explored in the context of freedom of information and individual privacy in Canada. Many turn up facts, acts, policies and procedures hitherto unknown to the general public.

In short, we feel that the Commission has done itself and the province a good turn by having these matters looked into and that we therefore have an obligation in the name of freedom of information to make them available to all who care to read them.

It goes without saying that the views expressed are those of the authors concerned; none of whom speak for the Commission.

D. C. Williams
Chairman

PREFACE

The terms of reference of this Commission raise for consideration one of the perplexing dilemmas of modern society. How is one to reconcile the apparent public interest in fostering a greater openness in the conduct of the affairs of public institutions with the public interest in the preservation of a social framework within which the individual's sense of personal privacy may be maintained? The perspective from which the Commission approaches this question is found in its central concern to make recommendations with respect to the fashioning of a policy relating to "the individual's right of access and appeal in relation to the use of government information."

A policy on public access to government information has at least two privacy dimensions. First, if the public is to be granted a broad right of access to government documents, what arrangements should prevail with respect to the public right of access to documents containing personal information? Should an individual member of the public be able to obtain copies of documents which contain personal information about another individual? If we assume that personal information should generally not be disclosed to others, are there circumstances in which the public right to know should take priority over the protection of the privacy of particular individuals? In short, how are we to avoid invading personal privacy under the banner of freedom of information?

The second privacy dimension to the right of access issue relates to the ability of an individual to obtain access to government files containing personal information about himself. As this research paper indicates, an increasingly large number of North American and European jurisdictions have adopted or are contemplating the adoption of statutory schemes which enable citizens to have access to personal files concerning them maintained by the government. The right of access is conferred in order to enable the individual to ensure the accuracy and fairness of the information contained in the file and to oversee the uses made of it. More generally, it is the purpose of such schemes to reduce the level of anxiety that might otherwise result from a lack of knowledge concerning the nature and contents of these personal files. An assessment of the desirability of such a scheme necessitates, in turn, a consideration of the broad range of privacy protection issues which arise in the context of the collection and use of personal information by the institutions of government. As will be seen, it is the authors' view that a right of access to government files is only one of a possible range of solutions to the privacy protection problem.

The increasing use of large and sophisticated information systems for the handling of personal data by both public and private institutions has stimulated much of the recent public discussion of privacy protection issues. A number of thorny questions now have a very familiar ring. What is the significance for the individual's "right to privacy" of the recent exponential growth in the capacity of computer technology and its various applications to personal information systems? How much information should be collected by the managers of such systems? On what terms and conditions should it be stored or disseminated? Should there be controls placed on the exchange of information between systems? What are the implications of the apparently increasing use of personal identifiers such as the Social Insurance Number by public and private data managers? In addressing problems of this kind, the granting of a right to "see the file" can make only a minor, albeit important, contribution.

This research paper has attempted to provide the Commission with a background of factual information and analytical discussion in order to assist the Commissioners in fashioning their recommendations with respect to these difficult questions. Limitations of time and resources have prevented the research team from embarking on a thorough and complete study of all personal record-keeping systems and practices of the government of Ontario. However, an attempt has been made to provide the Commission with a broad survey of the general nature of these practices together with a detailed account of the information systems employed in eight different areas of government activity. As well, the authors have given an account of the privacy protection schemes now in force in a number of other jurisdictions and have fashioned a set of recommendations of their own for the Commission's consideration.

The length of this research paper is eloquent testimony to the weight of the task undertaken by the authors and to the industry with which they have discharged their responsibilities. The greater part of the research which went into its preparation involved a time-consuming process of interviewing public officials in an attempt to provide, in most cases for the first time, an account of the manner in which personal information about the citizens of Ontario is employed by various ministries and agencies of the government. The authors enjoyed the cooperation of many public servants who gave freely of their time to participate in interviews, to check on the accuracy of interviewing notes, and to comment on draft chapters of this report. It is our hope, therefore, that the descriptive passages in this paper accurately reflect current practice in each of the areas discussed. It should be noted, however, that the preparation of this paper has occupied a period of approximately two years and it is entirely possible that the policies and practices of a particular public official or agency have evolved in some way from those portrayed here.

The research project which culminated in the preparation of this paper was supervised by Michael A. Brown, a former public servant in the government of Ontario who now engages in a consulting practice, in addition to his responsibilities as a Special Lecturer in Administration in the Administrative and Policy Studies Program at Trent University. Mr. Brown organized and initiated the research program in the spring of 1978 and worked on the project through to the early fall of that year.

Mr. Brown's co-authors have worked on the project since its inception and have continued the work of revision and preparation of the manuscript for publication while serving as members of the Commission's research staff. Ms. Billingsley, a graduate of the Master's Program in Sociology at the University of Toronto, carried the exclusive burden for the research and writing of the chapter on social services information systems and collaborated in the writing of many other chapters of the report. Ms. Shamai, a member of the Bar of Ontario and a graduate of Osgoode Hall Law School of York University, carried the primary responsibility of legal research and writing, together with a number of the case studies in Part B of the report. In the summer of 1978, Mr. Stan Kolankowski, a computer science graduate of the University of Toronto, assisted in the research relating to health information systems records.

The authors wish me to acknowledge, most gratefully, the assistance of others in the preparation of this paper. In particular, the advice received from a number of sources relating to the privacy implications of the use of computer technology was extremely helpful. Professor Steven Berkowitz of the Department of Sociology of the University of Toronto provided extensive revisions and advice with respect to Chapters IV and V of the paper. Professor Eric Manning, a computer scientist at the University of Waterloo, made a very helpful presentation to the Commission and to the research staff on the general subject of privacy and computers at an early stage of the Commission's work. As well, Professor Manning commented helpfully on an early draft of Chapter IV. Useful comments on Chapter IV were also provided by James E. Manning of the Computer Services Division of the Ontario Ministry of Government Services.

Finally, I wish to express the appreciation of the authors and of myself to Ms. Natalie Gold and Ms. Victoria Van Asperen for their contribution to the completion of this project. Ms. Van Asperen patiently endured and efficiently discharged the major portion of the secretarial tasks involved in the preparation of several drafts of the various chapters of the report. Ms. Gold performed a function, ably discharged with respect to other research staff publications as well, of helping the authors to refine their occasionally inaccessible prose into comprehensible form and more generally, in editing and supervising the preparation of the manuscript for publication.

(viii)

The Commission has resolved to make available to the public its background research papers in the hope that they might stimulate public discussion. It should be emphasized, however, that the views expressed in this paper are those of the authors and do not necessarily represent the views of the Commission.

Particulars of other research papers which have been published to date by the Commission are to be found on pages 644-645.

John D. McCamus
Director of Research

PRIVACY AND PERSONAL DATA PROTECTIONPART A: ISSUES AND ANALYSIS

| | | |
|-----------|---|-----|
| CHAPTER I | Introduction | 1 |
| II | Privacy and Data Protection | 7 |
| III | The Extent and Nature of Record-Keeping by the Ontario Government | 25 |
| IV | Computers and Government Records | 34 |
| V | Personal Identifiers: The Development of a Single Identifying Number | 65 |
| VI | Legislative Approaches to Privacy and Data Protection | 93 |
| VII | Conclusions and Recommendations to the Commission | 177 |

PART B: CASE STUDIES

| | | |
|------|--|-----|
| VIII | The Social Services | 218 |
| IX | Education | 372 |
| X | Government Personnel Records | 434 |
| XI | Health | 482 |
| XII | Law Enforcement | 530 |
| XIII | Corrections, Probation and Parole | 591 |
| XIV | Personal Property Security Registration | 615 |
| XV | Licensed Driver and Vehicle Ownership Records | 623 |

(x)

Detailed Table of Contents

PART A: ISSUES AND ANALYSIS

| | | |
|-------------|---|----|
| CHAPTER I | INTRODUCTION | 1 |
| CHAPTER II | PRIVACY AND DATA PROTECTION | 7 |
| | A. Informational Privacy | 15 |
| | B. Access to Records | 19 |
| | C. Conclusions | 22 |
| CHAPTER III | THE EXTENT AND NATURE OF RECORD-KEEPING BY THE ONTARIO GOVERNMENT | 25 |
| | A. The Basic Records | 25 |
| | B. Specialized Records | 27 |
| | C. Index of Personal Records | 29 |
| CHAPTER IV | COMPUTERS AND GOVERNMENT RECORDS | 34 |
| | A. The Computer's Effect on the Issue of Privacy | 34 |
| | B. The Development of Computer Systems | 40 |
| | C. Security of Computerized Records | 46 |
| | D. Technological Change and Privacy | 53 |
| | E. Automation of Personal Records in the Ontario Government | 55 |
| | F. Privacy and Computers | 63 |
| CHAPTER V | PERSONAL IDENTIFIERS: THE DEVELOPMENT OF A SINGLE IDENTIFYING NUMBER | 65 |
| | A. The Change from "Standard Identifiers" to Unique Personal Identifiers | 66 |
| | B. Single Identifying Numbers | 68 |
| | C. Personal Identifiers in the Ontario Government | 72 |
| | D. The Growing Use of the Social Insurance Number as a Single Identifying Number | 74 |
| | E. Solutions | 85 |

Detailed Table of Contents, cont'd ...

| | | |
|------------|--|-----|
| CHAPTER VI | LEGISLATIVE APPROACHES TO PRIVACY AND DATA PROTECTION | 93 |
| A. | The Tort Approach: Creating Private Rights of Action | 94 |
| B. | The Ombudsman Approach | 99 |
| C. | The Data Regulation Approach | 105 |
| 1. | General Description of Statutes | 107 |
| a) | Sweden | 107 |
| b) | France | 109 |
| c) | Federal Republic of Germany | 110 |
| d) | United States of America | 112 |
| e) | Canada | 115 |
| 2. | Collection and Storage of Personal Information | 116 |
| a) | Collection and Storage in Sweden | 118 |
| b) | Collection and Storage in France | 119 |
| c) | Collection and Storage in the Federal Republic of Germany | 120 |
| d) | Collection and Storage in the United States of America | 121 |
| e) | Collection and Storage in Canada | 124 |
| 3. | Transfer, Subject Access and Correction | 126 |
| a) | Transfer, Subject Access and Correction in Sweden | 130 |
| b) | Transfer, Subject Access and Correction in France | 133 |
| c) | Transfer, Subject Access and Correction in the Federal Republic of Germany | 136 |
| d) | Transfer, Subject Access and Correction in the United States of America | 142 |
| e) | Transfer, Subject Access and Correction in Canada | 150 |
| 4. | Enforcement and Administration | 154 |
| a) | Enforcement and Administration in Sweden | 156 |
| b) | Enforcement and Administration in France | 160 |
| c) | Enforcement and Administration in the Federal Republic of Germany | 162 |
| d) | Enforcement and Administration in the United States of America | 165 |
| e) | Enforcement and Administration in Canada | 169 |
| D. | Conclusions | 172 |

Detailed Table of Contents, cont'd ...

| | | |
|-------------|---|-----|
| CHAPTER VII | CONCLUSIONS AND RECOMMENDATIONS | |
| | TO THE COMMISSION | 177 |
| A. | General Conclusions | 177 |
| B. | Areas of Concern | 184 |
| | 1. Public Knowledge of Data Banks | 185 |
| | 2. Collection of Personal Information | 186 |
| | 3. Maintenance and Security | 187 |
| | 4. Transfer and Dissemination of Personal Information | 190 |
| | 5. Subject Access | 195 |
| C. | Recommendations | 197 |
| | 1. Alternatives Examined | 197 |
| | a) The Tort Approach | 197 |
| | b) The Data Regulation Approach | 197 |
| | c) The Fair Information Practices Approach | 198 |
| | d) The Public Awareness/ Ombudsman Approach | 199 |
| | e) The Freedom of Information Exemption Approach | 199 |
| | f) Internal Administrative Guidelines | 200 |
| | 2. Goals and Objectives | 201 |
| | a) Improving Public Knowledge about Government Record-Keeping | 201 |
| | b) Providing a Mechanism for Complaints, Research and Debate about Privacy Issues | 203 |
| | c) Encouraging Government Sensitivity toward Record-Keeping and Privacy Concerns | 203 |
| | d) Providing Record Subjects Privacy Rights | 204 |
| | e) Balancing Freedom of Information and Privacy Interests | 204 |
| | 3. Recommended Measures to Improve Personal Data Protection in Ontario | 206 |
| | a) To Increase Public Awareness of Government Information Practices | 206 |
| | b) To Facilitate Complaints and Research into Privacy Issues | 207 |
| | c) To Promote Government Agency Awareness of Privacy Issues | 209 |
| | d) To Assist Individuals in Protecting Their Privacy | 212 |
| | e) To Establish a Balance Between Data Protection and Freedom of Information | 215 |

Detailed Table of Contents, cont'd ...

| | |
|---|-----|
| <u>PART B: CASE STUDIES</u> | 217 |
| CHAPTER VIII THE SOCIAL SERVICES | 218 |
| A. Social Services for Adults | 222 |
| 1. Volume and Types of Records Held | 222 |
| 2. Record-Keeping Policies and Practices | 228 |
| a) General Protection of Privacy | 228 |
| b) Information Collection and Verification | 231 |
| c) Record Storage | 237 |
| d) Transfer of Personal Information | 240 |
| e) Research Access to Personal Files | 255 |
| f) Client Access | 257 |
| B. Social Services for Children | 263 |
| 1. Volume and Types of Records Held | 272 |
| 2. Record-Keeping Policies and Practices | 280 |
| a) General Protection of Privacy | 280 |
| b) Information Collection and Verification | 283 |
| c) Record Storage | 287 |
| d) Transfer of Personal Information | 293 |
| e) Research Access | 302 |
| f) Subject Access to Personal Records | 303 |
| C. Impact of Computerization on Privacy in Social Service Record-Keeping | 308 |
| 1. Data Collection | 312 |
| a) Client Awareness of Computerization | 312 |
| b) Collection of Subjective Data | 313 |
| c) Collection of Social Insurance Number | 315 |
| 2. Preparation of Data for Computerization | 316 |
| a) Editing/Correcting | 316 |
| b) Updating | 318 |
| c) Compilation | 319 |
| d) Key punching | 319 |
| 3. Computer Input, Storage and Output | 320 |
| a) Authorization of Personnel | 321 |
| b) Physical Security | 321 |
| c) Computer Security | 322 |
| 4. Distribution of Computer Generated Data | 323 |
| 5. Trend Toward Integration of Computer Systems | 324 |
| D. Conclusions | 327 |
| E. Alternatives | 336 |
| 1. To Decrease Volume and Types of Records Held | 339 |
| 2. To Revise Record-Keeping Policies and Practices | 344 |
| 3. To Ensure Subject Privacy in Computerized Social Service Personal Record Systems | 355 |
| Appendix VIII.A: Subject Access to Personal Records | 358 |

Detailed Table of Contents, cont'd ...

| | | |
|------------|--|-----|
| CHAPTER IX | EDUCATION | 372 |
| | A. Introduction | 372 |
| | B. Student Records | 373 |
| | 1. What is the OSR? | 377 |
| | a) The Record Folder | 378 |
| | b) The Student Achievement Form | 381 |
| | c) Miscellaneous Documents | 382 |
| | d) The Index Card | 382 |
| | e) Record of French Instruction | 383 |
| | 2. Legislated Access to the Record | 383 |
| | a) History of the Legislative Change | 385 |
| | b) Current Record-Keeping Practice with the OSR | 388 |
| | 3. Guidance and Psychological Reports | 391 |
| | 4. Medical Records | 397 |
| | 5. Other Contributors or Users of a Student's Record | 401 |
| | 6. Third Party Inquiries | 404 |
| | 7. Student Identification Numbers | 405 |
| | C. Teacher Records | 406 |
| | 1. Description | 406 |
| | 2. Access to Teachers' Files | 410 |
| | 3. Conclusions | 413 |
| | D. Universities, Colleges and Trade Certification | 414 |
| | 1. Description | 414 |
| | 2. Industrial Training and Trade Certification Records | 415 |
| | 3. Subject Access | 421 |
| | 4. Student Awards | 422 |
| | E. Conclusions | 430 |
| CHAPTER X | GOVERNMENT PERSONNEL RECORDS | 434 |
| | A. Introduction | 434 |
| | B. Organization of Employees | 435 |
| | C. The Hiring Process | 439 |
| | 1. Security Clearances | 442 |
| | D. Records Created During the Course of Employment | 447 |
| | 1. Computer-Held Files: IPPEBS | 449 |
| | 2. Manual Files | 455 |
| | a) The Corporate File | 456 |
| | b) Grievance Files | 458 |
| | c) Medical Records | 459 |
| | 1) General Health Records | 460 |
| | 2) Direct Services | 462 |
| | 3) Mandatory Referral | 463 |
| | 4) Record Storage and Security | 469 |

Detailed Table of Contents, cont'd ...

| | | |
|------------|--|-------|
| CHAPTER X | GOVERNMENT PERSONNEL RECORDS, cont'd ... | |
| | E. Access to Employee Records | 470 |
| | 1. Personnel Records | 471 |
| | a) Subject Access | 471 |
| | b) Transfers | 473 |
| | 1) Access by the Civil Service Commission | 473 |
| | 2) Access by the Employee Data Services Branch | 474 |
| | 3) Access Within Ministries | 474 |
| | 4) Access by Other Government Agencies | 476 |
| | 5) Access by the Public | 477 |
| | 6) Access by the Police | 478 |
| | c) Union Access | 479 |
| | 2. Grievance Files | 480 |
| | 3. Medical Records | 481 |
| CHAPTER XI | HEALTH | 482 |
| | A. Introduction | 482 |
| | B. Confidentiality of Health Records | 483 |
| | 1. Medical Records in the Primary Health Care Area | 486 |
| | a) The Need for Confidentiality in the Primary Health Care Area | 487 |
| | b) Results of the Erosion of Doctor-Patient Confidentiality | 489 |
| | c) Confidentiality and Subject Access | 491 |
| | 2. Supporting Activities: Medical Records Used by Health Care Service Payers and Health Care Reviewers | 494 |
| | 3. Non-Medical Users of Health Information | 496 |
| | C. Legislation Affecting the Confidentiality of Medical Records | 498 * |
| | 1. Mandatory Reporting Statutes | 499 |
| | a) Problems with the Reporting Statutes | 503 |
| | 2. Investigatory Statutes | 504 |
| | 3. Permissive Reporting Statutes | 508 |
| | D. Conclusions | 511 |
| | 1. Information Transfer and Dissemination | 511 |
| | 2. Subject Access | 514 |
| | E. The Health Care Number | 517 |
| | 1. The History of the Health Care Number | 518 |
| | 2. A Review of the Rationale for the Health Care Number | 522 |
| | 3. Privacy and the Use of the SIN in the Health System | 527 |

Detailed Table of Contents, cont'd ...

| | | |
|--------------|---|-----|
| CHAPTER XII | LAW ENFORCEMENT | 530 |
| | A. Introduction | 530 |
| | B. Organization of Policing in Ontario | 533 |
| | C. The Sources of Law Enforcement Information | 535 |
| | D. Systems of Personal Information | |
| | Record-Keeping by the Police | 539 |
| | 1. Introduction | 539 |
| | 2. Occurrence and Investigation Reports | 541 |
| | 3. Identification Files | 544 |
| | 4. Intelligence Files | 546 |
| | a) Criminal Intelligence | 547 |
| | b) Political or "Security" Intelligence | 553 |
| | 5. Criminal History Dossiers | 554 |
| | 6. The "Criminal Record" | 556 |
| | E. The Computerization of | |
| | Law Enforcement Information Systems | 562 |
| | 1. CPIC | 563 |
| | 2. ACIS | 568 |
| | F. Access to Law Enforcement Information | 570 |
| | G. Discussion and Conclusions | 576 |
| | 1. The Collection of | |
| | Intelligence Information | 576 |
| | 2. Disclosure of Law Enforcement | |
| | Information to Third Parties | 580 |
| | 3. Subject Access to | |
| | Law Enforcement Information | 583 |
| | 4. The Gathering of Law Enforcement | |
| | Information from Private and | |
| | Public Institutions | 588 |
| | 5. Computerization of Law Enforcement | |
| | Information Systems | 589 |
| CHAPTER XIII | CORRECTIONS, PROBATION AND PAROLE | 591 |
| | A. Policy on Confidential Information | 595 |
| | B. Inmate Records | 596 |
| | C. Probation Records | 600 |
| | D. Ontario Board of Parole | 606 |
| | E. Privacy Issues in Corrections | 608 |
| | F. New Developments | 613 |
| CHAPTER XIV | PERSONAL PROPERTY SECURITY REGISTRATION | 615 |

Detailed Table of Contents, cont'd ...

| | | |
|-------------|---|-----|
| CHAPTER XII | LICENSED DRIVER AND VEHICLE OWNERSHIP RECORDS | 623 |
| | A. The Licensed Driver File | 624 |
| | B. Vehicle Registration System | 632 |
| | C. Collision Reports | 636 |
| | D. Privacy Considerations | 637 |

Tables

| | | |
|-----------|---|-----|
| TABLE I.1 | Record Systems Examined by the Privacy Study Group | 4 |
| II.1 | Survey Carried Out by the Younger Committee | 9 |
| III.1 | Size and Content of Selected Ontario Government Personal Record Files | 31 |
| IV.1 | Ontario Manual of Administration Section 55.2.5 | 62 |
| VII.1 | Some of the People on Whom the Ontario Government Keeps Personal Records | 178 |
| VII.2 | Some Milestones in the Growth of Ontario Government Services | 179 |
| VIII.1 | Volume and Types of Social Services Personal Information: Selected Manual and Computerized Systems of Programs for Adults | 226 |
| VIII.2 | Ministry of Community and Social Services: Selected Programs for Adults, Signed Client Consent Forms for Information Transfer | 246 |
| VIII.3 | Types of Personal Information Transferrals from and to Ministry of Community and Social Services: Services for Adults | 248 |
| VIII.4 | Volumes and Types of Information Collected by Selected Records Systems of Childrens Social Service Agencies | 273 |
| VIII.5 | Information Transfers Between Selected Childrens Services and Three Domains | 298 |
| VIII.6 | Characteristics of Computerized Personal Record Systems in the Social Services | 310 |
| XI.1 | The Flows of Personal Medical Data | 485 |
| XI.2 | Canadian Health Record Association Code of Practice for Safeguarding Health Information | 512 |
| XV.1 | Ontario Classified Driver Licensing System Quick Check Chart | 625 |

CHAPTER I

INTRODUCTION

The purpose of this study, as set out in its terms of reference, is to report on the extent of, and need for, the protection of privacy in personal records maintained by the government of Ontario, and to assess the opportunities for citizen access to personal records. The end-product of the study is to determine whether generalized regulations and/or legislation governing privacy of personal records would be appropriate, and to provide suggested policies for each personal record area considered. Specifically, the study group was directed to examine personal records kept in the areas of education, health, social services, corrections, law enforcement and government personnel.

The study group, which consisted of four people with a variety of backgrounds in law, computer science, social services and administration, undertook the major part of its field research during the months of May, June, July and August, 1978. An important aspect of the work of the group involved a critical review of existing privacy legislation and implementation procedures both in Canada and abroad, and a review of selected literature in the field. However, the more significant part of the study was concerned with gaining a detailed understanding of how certain types of records about people are gathered, maintained and

disseminated by Ontario government ministries and agencies in each of the six areas with which we were concerned, with the exception of health. Because the Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario, under Mr. Justice Horace Krever, is carrying out an exhaustive investigation of record-keeping in the health field, we considered that our efforts would be redundant in this area and we have therefore simply summarized the major issues.

By taking this approach, which involved extensive interviews with administrators and operating staff at all levels, and in some cases with outside agencies and organizations to gain a different perspective, it was our hope that we would obtain a practical appreciation of the privacy concerns in each area. Since one of the major componenets of most privacy legislation is the right of access by a person to his/her file, we also wished to assess realistically whatever barriers might exist to completely open access to the data subject, and the impact which subject access might have on administrative and operational efficiency. Little work has yet been done in this area, and there have been few published evaluations of the impact of such legislation in jurisdictions where it has been implemented. Stories abound of reductions in program effectiveness, exhorbitant costs and the creation of underground networks to share information not placed on file. We are not, of course, examining record-keeping practices in an open access environment. However, we attempted to draw objective conclusions based on our examination of present record systems and to

extrapolate what might occur under a subject access scheme.

In considering Ontario government records, it is worth pointing out that where many of the legislative models we examined, such as the Canadian Human Rights Act, Part IV¹ and the United States Privacy Act, 1974,² concerned national agencies, a privacy scheme for the province would necessarily impact to a much greater extent on municipal records and the records of private agencies, because of the greater involvement of the province in direct service delivery. In most areas we could not conceive of a satisfactory privacy scheme which would apply only to provincial ministries and agencies. We did not, however, specifically attempt to examine municipal or private agency records, although we will comment when appropriate on the possible implications of province-wide legislation.

The report is in two parts. Part A deals with the conceptual problems in defining privacy, an overall assessment of record-keeping in the Ontario government and the use of computers, legislative approaches to privacy and data protection, and our conclusions and recommendations to the Commission. Part B covers the detailed results of the area surveys.

A summary of the record systems we examined is included in the table on the following page. In addition to the areas mentioned, we also briefly

1 S.C. 1976-77, c. 33.

2 5 U.S.C. s. 552a.

TABLE I.1

RECORD SYSTEMS EXAMINED
BY THE PRIVACY STUDY GROUP

Social Services

Adults:

Family Benefits
General Welfare Assistance
Vocational Rehabilitation
Mental Retardation

Children:

Children's Aid Societies
Adoptions
Child Abuse Register
Training Schools
Juvenile Probation
Mental Health Information System

Education

Student Awards
Pupil Records
Teachers Certification
Trade Certification

Corrections

Adult Inmates
Probation and Parole

Government Personnel

Pre-employment Records
Ministry Personnel Records
Integrated Pay, Personal and
Employee Benefits
Security Clearance Records

Law Enforcement

Canadian Police Information Centre
Criminal History
Criminal Occurrence
Identification
Intelligence

Others

Licensed Drivers
Registered Vehicles
Personal Property Security
Registration

examined three large record systems which did not fall strictly within the six areas suggested for examination in our terms of reference. All three were referred to us as being of special concern and deserving our attention. The Driver File and the Registered Vehicle File, which are both maintained by the Ministry of Transportation and Communications, were of interest because of their importance to law enforcement and because of concerns over the possible sale of personal information contained in them. The Personal Property Registration System in the Ministry of Consumer and Commercial Relations was examined because of specific privacy considerations with the personal information it contains.

It should be noted that it was not our intent to identify and investigate specific complaints of the abuse of privacy of personal records, although we were obviously interested in learning of such situations. Several such instances in fact came to our attention, although we did not actively invite them. Other commissions at both the federal and provincial levels are examining in detail situations where obvious abuses have occurred. These investigations will no doubt serve as object lessons for the public, government officials and politicians alike. We have been content to concentrate on describing the various environments in which records about people are assembled and used, in accordance with what we believe the Commission expects of us.

Finally, we would like to thank the large number of people in Ontario ministries and agencies, local government, the federal government, and

private agencies and business for their patience in answering our many questions and in helping us to understand the issue of privacy.

In conducting our study, we have been guided and aided to a considerable extent by studies in other jurisdictions, and particularly by the work of the Privacy Project Task Force which examined the issue of privacy in the Ontario context in 1976,³ and which led to the creation of this Commission. To the members of that group, we acknowledge a special debt of gratitude.

3 Ontario, Privacy Project Task Force: Report and Recommendations, Ontario Management Board of Cabinet (Toronto: July, 1976).

CHAPTER II

PRIVACY AND DATA PROTECTION

In order to consider the extent of an need for privacy of personal records kept by the Ontario government, it was obviously necessary for the study group to reach some understanding of the meaning of the term "privacy," particularly in the context of personal information. The difficulties involved in defining "privacy" quickly became apparent to us, however, as we looked at the experience in other jurisdictions. Attitudes to privacy apparently vary from country to country and from person to person, and can change over time. A recent poll in the United States¹ indicated that 71% of Americans agree that they "begin surrendering their privacy the day they open their first charge account, take out a loan, buy something on the installment plan or apply for a credit card." In 1974, only 48% felt the same way. A 71% majority also now believes that it is common practice for "the government to say whether or not a person can look at files" collected on that person, and 60% view this as a "very serious" violation of individual privacy. This is in spite of the fact that since 1974, Americans have had a legislated right of access to federal government files under the Privacy Act,² and many states also have similar acts.

1 Harris Survey, June 15, 1978.

2 5 U.S.C., s. 552a.

In Britain, the Younger Committee³ produced some interesting statistics on the relationship between attitudes to privacy and age (see Table 1). They indicate that privacy becomes less of a concern with age.

Finally, the following two examples of privacy issues in other countries illustrate the wide variety of attitudes and approaches to the problem, and the need to examine the issue in the context of current societal values.

1) In 1970, the French government introduced two bills to reinforce traffic safety by integrating information held by the Ministry of the Interior (on drivers' licences) with that of the Ministry of Justice (on convictions for traffic offences). In the integrated register, drivers would be classified according to a scale of penalty points for traffic offences, and information from the register would be provided (among others) to private insurance companies. After considerable debate, the government's proposal to entrust custody of the registers to a special agency was rejected, and for the sake of protection of civil liberties, the Parliament was adamant in asking that the two registers outlined in the law would not be simply interconnected. Safeguards were introduced for guaranteeing the rights of persons concerned and limiting access by others.

3 Report of the Committee on Privacy (Cmd. 5012, 1972) Appendix E, Table 24.

4 Hondius, Frits, Emerging Data Protection in Europe (New York: American Elsevier Publishing Co., 1975) 31-33.

TABLE II.1

SURVEY CARRIED OUT BY
THE YOUNGER COMMITTEE

Number objecting to publication
of various personal details, by age:

| | | Age | | | |
|----------------------------------|-------|-------|-------|-------|-----------|
| | | 18-30 | 31-44 | 45-64 | 65 & Over |
| Weighted number of interviews | 1,596 | 377 | 410 | 533 | 263 |
| Would object to availability of: | (%) | (%) | (%) | (%) | (%) |
| Address | 33 | 39 | 32 | 31 | 29 |
| Telephone number | 34 | 40 | 33 | 32 | 34 |
| (Wife's) maiden name | 18 | 23 | 15 | 19 | 18 |
| Nationality | 8 | 12 | 6 | 8 | 6 |
| Racial origin | 10 | 14 | 7 | 10 | 6 |
| Occupation | 12 | 20 | 12 | 9 | 9 |
| Education | 17 | 28 | 16 | 14 | 8 |
| Political views | 42 | 58 | 44 | 36 | 27 |
| Religious views | 28 | 48 | 27 | 20 | 12 |
| Leisure activities | 22 | 34 | 25 | 17 | 9 |
| Income | 78 | 89 | 80 | 73 | 66 |
| Sex-life | 87 | 95 | 90 | 84 | 75 |
| Medical history | 51 | 59 | 59 | 48 | 34 |

2) In 1973, Belgium commenced the operation, on an experimental basis, of a "Register National" containing information about 8 million of the country's 9.7 million population and 130,000 corporate enterprises in an integrated central data base. The Register uses personal identification numbers and contains information on names, date of birth, sex, family, present and former residence, and profession. Even more extensive information is kept about aliens. The data bank is used not only by public authorities, but also increasingly by private parties.⁵

Almost all Western nations are now grappling with problems of privacy, particularly with regard to personal data, but their starting points and their specific concerns differ significantly. The use of the Social Insurance Number and other identifiers is a topical matter of debate in Canada. In the United States, extension of the use of the Social Security Number (SSN) has been expressly prohibited.⁶ This is very

5 Hondius, op. cit., 27-28.

6 Privacy Act, U.S. Public Law 93-579; s. 7 reads as follows:

(a)(1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

(2) the provisions of paragraph (1) of this subsection shall not apply with respect to --

(A) any disclosure which is required by Federal statute, or

(B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(cont'd)

different from the Belgian acceptance of a national data base containing individual identity numbers. In Ontario, the Driver Licence File has contained information about traffic convictions and demerit points for many years. This information has traditionally been available to the police and to insurance companies, even before the computerization of the file. Undoubtedly, some French administrators wish they had integrated their files before concerns for privacy became so vocal.

In Ontario, there is no legal right of privacy, and until the introduction of the Canadian Human Rights Act, Part IV, there was no definition of the term in federal legislation. Although British Columbia,⁷ Manitoba,⁸ and Saskatchewan⁹ have established a tort for invasion of privacy, actionable without proof of damage, these statutes are not of significant assistance in defining privacy of information collected about people.¹⁰

6 (cont'd)

(b) Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

7 Privacy Act, S.B.C. 1968, c. 39.

8 Privacy Act, S.M. 1970, c. 74.

9 Privacy Act, S.S. 1974, c. 80.

10 Only one case has yet been reported under any of the three statutes. Davis v. McArthur (1971) 17 D.L.R. (3d) 760.

The development of a definition of privacy has been a long and difficult process for all nations. The various attempts to refine and specify the context of this notion have not yet reached a general consensus. The ambiguous and elusive nature of the concept has frustrated the attempts of legislators and scholars to give clear guidance as to what we mean to protect when we wish to insulate individuals from an invasion of their privacy.

It was clear to us that little would be gained from our spending much time debating the question of what privacy is, much less what is the right to privacy. More eminent men and women than we have grappled with the problem and given up.¹¹ To quote from the Younger Committee report from Great Britain:

The majority of us regard the "Justice" Committee's conclusion as one more indication, and a highly significant one, that the concept of privacy cannot be satisfactorily defined. We have looked at many earlier attempts, and have noted that there are important differences between them all. Either they go very wide, equating the right to privacy with the right to be let alone, or they boil down to a catalogue of assorted values to which the adjective "private" or "personal" can reasonably, but not exclusively be attached. We conclude from these manifold efforts that no useful purpose would be served by our also entering the lists with yet another attempt to formulate a precise and comprehensive definition of privacy. 12

While we agreed with this statement, we did however believe that it would be useful to summarize briefly the various attempts that have been made

11 British Section of the International Committee of Jurists, "Privacy and the Law," referred to at Report of the Committee on Privacy (Younger Committee) (Cmd. 5012, 1972) 17.

12 Ibid.

to define privacy, and the state of current thinking on the subject as it relates to informational privacy. Finally, we wanted to reach some framework for analyzing the study findings, even if we could not precisely define its central concept.

There have been many attempts to define privacy in a workable fashion that would enable a legal right to it to be established. Some writers have characterized privacy as a space surrounding a person which should remain inviolate unless voluntarily yielded up by the individual.¹³ Absolute privacy would mean a total withdrawal from contact with others, and for most people this is clearly undesirable and in any case, impossible to achieve. Privacy, therefore, involves establishing a balance between closedness and openness, and the right to privacy is the individual's right to determine where that balance lies. Where the right does not exist, it is presumably society at large that in some way draws the dividing line in terms of its need for knowledge or its need to influence the person in some way.

The most consistent attempts to reach a definition of privacy have taken place in the United States, beginning with Judge Thomas M. Cooley,¹⁴ who first noted in 1888, "a right to be let alone." He was quickly followed by Samuel Warren and Louis Brandeis,¹⁵ who crystallized the

13 Altman, Irwin, Privacy Regulation: Culturally Universal or Culturally Specific? (1977) 33 Journal of Social Issues 66.

14 Cooley, Treatise on Torts, (1888).

15 Warren, Samuel D. and Brandeis, Louis D., The Right to Privacy, (1890) 4 Harvard Law Review 289.

argument which redefined common law property rights as they applied to personal writings and other productions as a principle of "inviolable personality." This imprecise definition of the "right to be let alone" as a protection of man's "inviolable personality" was hardly a satisfactory basis for legal construction and application, and there have been many attempts to improve upon the definition since then. Some analysts concluded that there is no independent privacy interest and hence no single right of privacy.¹⁶ Others attempted to develop generalized theories of individual privacy, to reconcile divergent trends in case law.¹⁷

A more fundamental approach which perhaps gets to the heart of the matter, but which, although it adds to an understanding of privacy, does not directly assist in formulating a privacy right, was taken by Charles Fried. He saw privacy as providing a "rational context" for "a number of our significant ends in life," such as love, trust, friendship, respect and self-respect:

Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable. They require a context of privacy or the possibility of privacy for their existence. To make clear the necessity of privacy as a context for respect, love, friendship, and trust is to bring out also why a threat to privacy seems to threaten our very integrity as persons. To respect, love, trust, or feel affection for others and to regard ourselves as the objects of love, trust and affection is at the heart of our

16 Prosser, William L., Privacy, (1960) 48 California Law Review 383.

17 Bloustein, Edward, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, (1969) 39 New York University Law Review 962.

notion of ourselves as persons among persons, and privacy is the necessary atmosphere for these attitudes and actions, as oxygen is for combustion. 18

A. Informational Privacy

Current concerns over privacy have increasingly centred around the need to control personal information, and the use of the term "information" has enabled more precise definitions of privacy to emerge, at least insofar as that aspect of "inviolable personality" is concerned. Probably the most well-known definition of privacy in its informational context is that proposed by Dr. Alan Westin, who defined it to be:

... the claim of individuals, groups and institutions to determine for themselves when, how and to what extent information about them is communicated to others. 19

This definition, however, is stated as a claim which is often overridden by social needs. It is a claim in the context of present-day society, in which essential services (particularly in urban areas) are organized, funded and delivered collectively, and for the running of which information about individual members of the collectivity is a requirement. The ramifications of informational privacy therefore go beyond simple considerations of control over data, and have profound

18 Fried, Charles, An Anatomy of Values (Cambridge, Mass: Harvard University Press, 1970).

19 Westin, Alan, Privacy and Freedom (New York: Atheneum, 1967).

implications on the types and extent of collective decisions. Privacy, as it relates to the provision, manipulation and control over information, is a political issue in that decisions over what information shall or shall not be collected about people can dictate the extent, nature or cost of the service, and in some cases whether the service is to be provided at all. For example, advocacy of the use of computers and of a unique personal identifier is often based on grounds of reduced costs. Some societies have foregone those cost-savings in order to ensure that privacy is not unduly invaded.²⁰

Since information flows between one person and the next, it is quite easy to conceive, as Westin has done,²¹ informational privacy as a definition of those pieces of information about a person that should or should not flow to others. However, putting the concept into practice presents considerable problems because views differ as to exactly what information flows should be prohibited. Those views are subject to change with changing individual and social circumstances.²² Westin's definition raises but does not solve the problem posed by the realities

20 Privacy Act, U.S. Public Law 93-579, s. 7. As of 1974, it was illegal for American authorities at the federal, state and local levels to deny benefits provided by law because of an individual's refusal to disclose his social security number, unless such disclosure was required by law. When disclosure is requested, the voluntary or mandatory nature of the request must be revealed also.

21 Westin, op. cit.

22 O'Brien, David, Privacy and the Right of Access: Purposes and Paradoxes of Information Control (1978) 30 Administrative Law Review 45.

of our present-day society in which services are organized, funded and delivered collectively in such a way as to make essential the recording and use of personal information about individual members of the society.

In one sense, the decision as to when, how and to what extent information about individuals is communicated to others is therefore made collectively rather than by individuals. Though the individual citizen does, in most cases, have the option of not providing information, the penalties for not doing so are so great (e.g. not being able to drive a car, obtain credit, etc.), that there is no effective personal control over the collection of personal information. The individual has, in substance, lost control over whether or not information shall be collected about him/her, even though s/he is frequently the primary source of that information. If the decision to gather personal information is taken by society, however, we must also note that this has seldom been a conscious decision taken after open public debate. Indeed, it is most often the administrators of government programs who will establish the informational requirements. In the private sector it will be a managerial decision as to what information is needed to provide the products and services society demands, or at least, are purchased by the consuming public. Individuals seldom have the opportunity to present their views on whether or not such data collection amounts to an unwarranted invasion of their privacy.

This is precisely why privacy is coming to be of such concern in almost all nations of the western world. The explosion of information

collection has paralleled the tremendous growth in public and private services, and it is doubtful if many of these services could have been provided without a firm foundation of information about the people who use them. Considerations of privacy, however, may not always have been fully addressed, if at all, in setting up systems for data collection. The rapidly expanding use of computers has compounded misgivings about what is, or might be, done with the information.²³ Part of the concern for informational privacy, therefore, stems from the fact that although people know that a lot of data is being collected, they don't know what is happening to it. Moreover, they fear that technological capacity or development may influence the way in which data is controlled or used, and may generate practices that may be harmful to their privacy interests.

Attempts to provide protection in legislation against invasion of privacy have therefore taken two directions. The first is the establishment of some kind of body to oversee data collection activities,²⁴ or to monitor possible instances of privacy invasions.²⁵ In some cases, this has involved requiring the registration of data collectors,²⁶ particularly those who use computers, and also

23 Miller, Arthur R., Assault on Privacy (Ann Arbor: University of Michigan Press, 1971).

24 Land Hessen (Federal Republic of Germany) Data Protection Act, 1970, Translation in Sieghart, P., Privacy and Computers (London: Latimer, 1976) 160.

25 This is the function of the New South Wales Privacy Committee.

26 As with the Data Inspection Board in Sweden, created by the Swedish Data Act in 1973.

stipulating the kinds of information (race, religion, political affiliation) prohibited from collection. The second step is the setting up of measures in law which are designed to protect data, once it has been collected, from misuse. In these latter schemes, it is the individual who is given the major responsibility, along with certain rights, of ensuring that these measures are enforced.²⁷

B. Access to Records

The starting point in considering any personal data protection scheme must therefore be the premise that the individual has an overriding interest in that data and how it is used and maintained. Given that individual privacy has been invaded in the first place -- even if the person concerned willingly yields up the information -- governments, and indeed all gatherers of personal data, must surely acknowledge a responsibility for the safekeeping of that data.

There are three main ways in which such a responsibility might be abrogated and against which protection is required:

- 1) The data may be wrong. It may have been recorded incorrectly or it may simply be incomplete or out-of-date.
- 2) The data may not be secure. Leaving aside the question of public access to personal data for the time being, the data may fall into the hands of others for whom it was not intended.
- 3) The data may be passed on to others for whom it was not intended, and used for purposes other than those for which it was gathered in the first place.

27 Canadian Human Rights Act, S.C. 1976-77, c. 33; U.S. Privacy Act, 1974.

It should be noted here that anyone may be subject to the harmful consequences of such errors or abuses, no matter where one stands on the issue of privacy.

Most privacy legislation, therefore, embraces to varying degrees certain basic principles for data protection, which have been most clearly stated in the U.S. Department of Health, Education and Welfare Report entitled, "Records, Computers and the Rights of Citizens." The report suggested a Code of Fair Information Practice as safeguard requirements for automated personal data systems:

There must be no personal data record-keeping systems whose very existence is secret.

There must be a way for an individual to find out what information about him is in a record and how it is used.

There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

There must be a way for an individual to correct or amend a record of identifiable information about him.

Any organization creating, maintaining, using, or disseminating records or identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. 28

To breathe life into these principles obviously means providing access by individuals to their own records. With certain exceptions, most records are made accessible in privacy legislation.

28 U.S. Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens (Cambridge, Mass: Massachusetts Institute of Technology, 1973) 40.

Concurrent with concerns for individual privacy, many jurisdictions are also considering, or are implementing, freedom of information legislation. Whereas privacy legislation can cover personal data held by both public and private organizations, freedom of information legislation is directed at opening up access to government files which may contain personal data. There is a problem, therefore, in reconciling privacy and the public's desire for information:

For any individual, privacy, as a value, is not absolute or constant; its significance can vary with time, place, age and other circumstances. There is even more variability among groups of individuals. As a social value, furthermore, privacy can easily collide with others, most notably free speech, freedom of the press, and the public's "right to know." 29

The difficulties involved in reconciling these two opposing requirements are illustrated by the experience in the United States with the Privacy Act of 1974 and the Freedom of Information Act amendments of the same year.

Although provisions of each Act significantly regulate administrative discretion, together the Acts do not supply an adequate information policy for reconciling both interests in privacy and access. The Freedom of Information Act encourages agencies to err on the side of disclosure by allowing disclosures, while neglecting to provide for incentives to safeguard personal privacy. The Privacy Act permits disclosures only when required, but does not supersede the Freedom of Information Act. Furthermore, administrative compliance is uncertain, if not impossible, because of the conflicting requirements of the Acts. 30

The Freedom of Information Act specifies that information may be exempted

29 Ibid.,

30 O'Brien, op. cit., 87.

from disclosure to a third party if it contains personal data, the release of which would be a "clearly unwarranted invasion of privacy."³¹ Of course, this brings us full-circle back to the need to define privacy, and more than this, the need to define what is meant by a clearly unwarranted invasion of it.

There is, however, a correlation between concerns for informational privacy and concerns for access to government documents; both involve the right of individuals to control information important to their governance. Access by people to their own records is held by some to be a limited version of general access to government files. The two Acts were intended by the U.S. Congress to establish a balance between privacy and the public's right to government information. However, the Privacy Act does not supersede the provisions of the Freedom of Information Act and it cannot be concluded that Congress has succeeded in its intention. The paradox between the two types of access and the confusion it creates remains.

C. Conclusions

After following in the literature the course of the debate on privacy and the outcome of this debate in several countries in the form of privacy legislation, it seemed to us that four fundamental conclusions could be reached, on which to base our study. They are as follows.

31 5 U.S.C. s. 552(b) (6).

1) Privacy has not been satisfactorily defined, although the attributes of data protection have been adequately stated in the "Code of Fair Information Practice" of the American Department of Health, Education and Welfare. We subscribe to these principles.

2) It is nonetheless important to provide a means to help people to reach agreement on where an invasion of privacy is unwarranted, i.e., the balance between individual control over personal information and the need of society to have that information. The balance may change as values, attitudes and social and individual circumstances change. If the problem of striking such a balance is left only to those whose primary interest is the gathering and use of personal data, there is some peril that the privacy concern will not be fully addressed. An opportunity should therefore be provided for individuals to participate in the process of determining where the balance should lie.

3) The central principle for protecting personal information is the notion that the individual should be able to assure him/herself that the "Code of Fair Information Practice" is being adhered to.

4) In providing to individuals the right to ensure that data is being protected, there is another question of balance which concerns the necessity for society to protect itself and to afford protection to sources of information it obtains about individuals.

Our examination of Ontario government record-keeping practices was

therefore aimed at determining how these four points are to apply in Ontario ministries and agencies. In the case of points (3) and (4), it is obviously possible on some issues for a very strong consensus to emerge on where the balance should lie. It then becomes possible to establish firmly in law what specific information shall or shall not be collected or made accessible. Examples of this can be seen in the existing data protection legislation (a term we prefer to use over privacy legislation) of other countries. These are discussed in Chapter VI, in which we explore the different approaches to privacy protection, which are many and varied.

CHAPTER III

THE EXTENT AND NATURE OF RECORD-KEEPING BY THE ONTARIO GOVERNMENT

One of the first questions people ask about government record-keeping is "what do they have on me?" The purpose of this chapter of the report is to briefly give some answers to that question as a background to the studies of specific areas of record-keeping which are detailed in Part B. The answer depends, of course, on who you are -- your age, education, occupation, income and interests. A real estate broker who is married to a teacher, owns property, has a university degree, and drives too fast will have more on file about him/her than someone who is single, works as a store clerk, rents an apartment and whose main pleasure is watching television.

A. The Basic Records

The Ontario government has some information about nearly all of us, with very few exceptions, which can be readily retrieved by name. If we were born in Ontario, the record will have begun with the registration of birth by the Registrar General. During our childhood, our schools will have collected substantial information about us, and through our parents our names will appear in the Ontario government Ministry of Health records, which will contain a notation about our

visits to the doctor and major illnesses. In addition, the Ministry of Health may have information about us from school health records. It is when we leave school to start a job or to go to university, however, that the number of records begins to multiply. Student loans, taxable income, driver's licences, car ownership, consumer loans, all create records about us. These records are all held separately by various agencies of the government. Some of these files are public, for example:

- 1) Assessment rolls available from municipal offices which give the name of everyone living at a given address, the name of the owner and a description of the property;
- 2) Driver records which include the name, date of birth and address of everyone who is licensed to drive a vehicle in Ontario, together with driving convictions, suspensions and demerit points;
- 3) Registered vehicle records which include the name and address of owners of vehicles;
- 4) Personal property registered as security against a loan which includes the value of the secured property, the name and address of the debtor, and sometimes the date of birth.

It is therefore possible to find out where someone lives, the person's age, what car s/he drives or what loans may be outstanding, directly from Ontario government records. However, a name is a poor identifier because of similarities between names, and the person searching these records would also need to know the whereabouts of the person they were interested in or their approximate age. Alternatively, the car licence number plate alone may give sufficient information to be able to trace a person back through all four files.

Other basic information is of a more confidential nature. The Ministry

of Health collects extensive data on patients from physicians and hospitals, and maintains a large file on the medically-insured population of the province in order to administer the OHIP system. The Ministry of Revenue obtains personal income tax data from the federal government for fiscal planning purposes. The Registrar General maintains records of births, marriages and deaths. Release of information from these files is governed by statutory confidentiality provisions.

B. Specialized Records

As we have mentioned, beyond these basic kinds of records which exist for almost every person in the province, the number of types of records about a person kept by the Ontario government depends on an individual's activities or the problems s/he encounters. Many businesses and professions are regulated. Teachers, realtors, car salesmen, projectionists, travel agents, private investigators, and security guards (among others) all have records kept about them. Everyone who seeks a grant or loan from the government, such as farmers, students, and businessmen has a file opened. In most cases, such files contain factual information about financial status, occupation, dependants, education, etc., but some files may also include a physical description and a notation as to criminal history, if any. In the majority of situations, this information is provided directly by the individual

concerned, although it may be checked against other sources. The person is often informed if this is to be done.

Those in need of assistance from government or whose actions government is responsible for controlling, have the most extensive records collected about them. Such assistance is usually subject to some kind of assessment of need, and eligibility has to be established and monitored. When the law is broken, offenders have to be traced and guilt proven. A penalty may be imposed, and this is often determined on the basis of the individual's past behaviour, history and personal circumstances, all of which are explored in considerable detail. During this process, information about or obtained from the person's family members, friends and employers may be included in the record. In some cases, a psychiatric report may be ordered.

We have so far discussed records created in order to regulate people's activities or to grant a benefit or deliver a service. Records may also be created, however, to provide information used by government in planning or research. Census data is the most obvious example of personal information collected purely for statistical research purposes, but some ministries regularly gather their own information. For example, the Ministry of Industry and Tourism collects data about travellers who visit their travel information centres in order to determine the travel patterns and interests of tourists in the province. The Ministry of Labour gathers data about workers in Ontario

from such sources as Canada Manpower Centre registration forms. In addition, planning and research groups within ministries may make use of information which is collected routinely in the administration of government programs.

C. Index of Personal Records

There were several sources on which we drew to make our assessment of the extent of personal records kept by the Ontario government, none of which proved entirely satisfactory. Within each ministry a schedule of all records is kept in document or microfilm form. The purpose of the schedule is to control the preservation and destruction of government documents, and the schedule contains lists of all physical collections together with a description of the particular collection of records and its size. However, although the Commission attempted to develop a comprehensive list of records from the schedules, it was unable to produce an accurate listing, nor to identify from that listing those records specifically containing personal information. The main problem was that record schedules are compiled by the ministries to control documents, and not to provide a compilation of record collections for analysis purposes.

Another source of information about personal records is the electronic data processing (EDP) systems plans submitted by ministries to the Management Board as part of the process of preparing annual financial

estimates. These plans describe all operating and proposed computer systems. Their purpose and major orientation in terms of the type of record and the data would provide a good basis for an index of computerized personal record systems, although the purpose of the plans is financial rather than to tabulate computer systems.

Perhaps the best publicly available indication of the extent of personal record-keeping by the Ontario government is the Catalogue of Statistical Files, which is published by the Ministry of Treasury, Economics and Intergovernmental Affairs. The Catalogue includes a somewhat arbitrary selection of files, many of which contain personal records and where available, the size of each file is noted. Some important personal record files which would presumably be useful from a statistical standpoint are missing from the Catalogue, while others which are included are of dubious statistical value. An attempt is also made to indicate the confidentiality of the information, although the categories used do not appear to conform with any standard and are inconsistently applied. In spite of its limitations, however, the publication is an interesting document because of the overview it provides of the wide scope of personal records maintained by the Ontario government.

A selection of personal record files together with their relative sizes are given in the Table on the next page, as an indication of the range of records kept by the government. Information included in the table, which also indicates the content of the respective files, was taken from

TABLE III.1

| SIZE AND CONTENT OF SELECTED ONTARIO GOVERNMENT PERSONAL RECORD FILES | | Date of Birth | Current Address | Education | Occupation or Employment | Property and Assets | Income | Medical | Criminal Offences | Family Details | Physical Description |
|---|---------------------------|---------------|-----------------|-----------|--------------------------|---------------------|--------|---------|-------------------|----------------|----------------------|
| | Approx. no. of Records | | | | | | | | | | |
| Vital Statistics | 8,000,000 | x | | | | | | | | x | |
| Licensed Drivers | 5,000,000 | x | x | | | | | x | x | | x |
| Vehicles and Owners | 5,000,000 | | x | | | x | | | | | |
| OHIP Subscribers | 8,000,000 | x | x | | | | | x | | x | |
| Student Health Records | 600,000 | x | x | | | | | x | | x | |
| Physicians | 14,000 | x | x | x | | | | | | x | |
| Nurses | 90,000 | x | x | x | x | | | | | | |
| Business Registration | 40,000 | x | x | x | x | x | x | | x | x | x |
| Property Registration | n/a | x | x | | | x | | | | | |
| University Students | 230,000 | x | | x | | | | | | x | |
| Teachers | 212,000 | x | x | x | x | | x | x | x | x | |
| Government Employees | 75,000 | x | x | x | x | | x | x | | x | |
| Public Housing Tenants | 56,000 | x | x | | | x | x | | | x | |
| Welfare Recipients | 135,000 | x | x | x | x | x | x | x | x | x | x |
| Provincial Child Wards | 13,000 | x | x | x | | | | x | x | x | x |
| Criminal Histories (OPP) | 400,000 | x | x | x | x | | | | x | x | x |
| Correctional Inmates | 400,000 | x | x | x | x | | | x | x | x | x |

our individual interviews, annual reports, and the Catalogue of Statistical Files. It should be noted that the degree of detail in the different types of records varies significantly according to the nature and use of the record. For example, "family detail" in most cases is merely a notation of marital status, but in the records of children who are wards of the province, this may extend to a detailed description of parental relationships and attitudes.

We would like to have made a better quantitative estimate of the extent of record-keeping in the Ontario government, but it was impossible to develop a satisfactory assessment. In our interviews, we examined in some detail approximately 30 separate types of record systems. A review of computerized systems containing personal information gave a figure of 117 systems operating or currently under development. Some of these are quite small, while others are very large. There are, of course, many more manual file systems which often back up what is on computer. They are spread right across the province in head offices, regional offices, and field offices. Wide variations in the size of different record systems make it meaningless to provide tabulations and percentages of files or systems containing various types of personal information. One would have to begin with a total of the number of individual personal records kept by the government, and this is a figure which is simply not available. In addition, to say for example, that 30% of systems contain "sensitive" information (for want of a definition, more than just name, address and date of birth), would ignore the fact that some systems may contain millions of records about

people, while others contain only thousands of records, and would therefore give a false and inaccurate impression. Also, even a name on a certain file may be highly sensitive.

A full accounting of the extent of Ontario government personal record-keeping would require a concerted effort on the part of all ministries and agencies, and could be produced in a relatively short period of time. The federal government has, of course, produced an Index of some 1,700 federal data banks -- Ontario could obviously do the same. We did not believe it was within the scope of our study or our resources to do more than explore currently available sources and comment on their limitations.

CHAPTER IV

COMPUTERS AND GOVERNMENT RECORDS

A. The Computer's Effect on the Issue of Privacy

Although government agencies, and indeed all large organizations which deal with people, have always collected personal information, it was the widespread use of computer-readable files which triggered the controversy over the privacy and security of these records. In the popular imagination, and to some extent the popular press, the computer was seen to be the villain of the piece because it greatly increased the capacity of governments to store, manipulate, analyze, and communicate large volumes of information. This, in turn, raised the spectre of a society in which every significant act or transaction of an individual would become a matter of public record or concern. Moreover, given the difficulties inherent in protecting personal records in government hands, computerization led to the widespread feeling that the vulnerability of individuals to unauthorized or illicit use of these records had palpably increased.

These developments, however, must be understood in context. During the 1960's, there was an enormous increase in the demands upon government

to regulate the economy, reduce social inequality, eliminate discrimination, and to "cure" other social ills of the time. In short, government programs came to be seen as the principal mechanism through which society, as a whole, could shape and direct its future. In order to perform this task effectively, it became necessary, in turn, for government to rapidly increase both the sheer volume and the range of the information which it collected about individual citizens, corporations, voluntary organizations, and other institutions.

Given these developments, and given the societal and cultural introspection which were another hallmark of the 1960's, there were strident cries of alarm about the dangers which computerization might pose to individual privacy and freedom. These warnings were most persistent in the United States, given the serious prospect of the creation of a national data bank which was to have encompassed almost all non-security related federal data systems.

Expert opinion on the extent to which computer-based technology, in and of itself, represents a distinct threat to the fabric of democratic society was and is divided. On the one hand, there is no doubt that the simple existence of an information storage and retrieval tool as powerful as a modern computer greatly increases the capacity of government to utilize, for well or ill, the information which it collects. On the other, however, the chief effect of computerization has been to increase efficiency in the handling of personal data by

government. The gathering of these data is still largely done by non-electronic means and is expensive and time-consuming. Moreover, data which have not been gathered cannot be manipulated and the content of computer-readable files -- the range and character of the data they contain -- is an independent question. Thus, while current computer technology makes it possible to assemble a detailed dossier on every citizen, to track significant acts or transactions in which s/he may engage, and to store and retrieve these data relatively easily, autocratic states have been and are able to accomplish this without the use of computers. The public policy decision to assemble bodies of information of this kind, moreover, has not, as a rule, been taken in countries with the ready access to advanced computer technology, but where the use of such technology is not widespread, e.g., in the Soviet Union, parts of Latin America and the Middle East. At the very least, this would suggest that computerization and the autocratic use of personal information do not necessarily go hand in hand.

Another source of popular concern has been the apparently exponential increase in the adoption of computer-based technology by retail companies, banks, public utilities, insurance companies, etc., during the 1960's and 1970's. Controversies regarding the computerization of these records have frequently reflected a fear that they might be used by private, governmental, or quasi-governmental agencies for surveillance purposes and/or to deny individuals access to employment, credit, etc.

While there has been general agreement that there are no insuperable technological barriers to the use of computerized data files in these ways, there is little evidence of movement in this direction at present.

A study conducted by Alan Westin of 55 governmental, commercial, and non-profit organizations in 1972 concluded that:

Computer usage has not created the revolutionary new powers of data surveillance predicted by some commentators. Specifically, the great majority of organizations we studied are not as a result of computerizing their records, collecting or exchanging more detailed personal information about individuals than they did in the pre-computer era. They are not sharing identified information more widely among organizations that did not carry out such exchanges in the pre-computer era.

1

Westin cites four impediments characteristically encountered in the integration of data systems both within and between organizations:

- a) the need to reorganize bureaucratic structures in order to fully utilize computer-based technology;
- b) the necessity for a clear articulation between the goals, programs, and decision-making patterns within an organization and the design of its data system;
- c) the high marginal cost of implementing new computer systems while continuing to gather and utilize data in a more traditional fashion; and
- d) the divergent programming requirements of different potential users of central data banks.

2

Interestingly, two of these impediments have been largely removed through technological advances which have occurred in the period since

1 Westin, Alan, Databanks in a Free Society (New York: Quadrangle, 1972) 341.

2 Ibid., 238-240.

Westin concluded his study. The cost of implementing new computer systems has been greatly reduced through the introduction of pre-packaged systems which have been built so as to accommodate a variety of users with widely divergent intended uses in mind. Moreover, the most advanced systems of this kind have been designed so that they can be accessed by persons with only minimal programming skills.³ These so-called "data base management systems" are described in detail in the next section.

From this we may infer that, to the extent that constraints still exist which impede the integration of data systems within and between organizations, these are primarily of two kinds; organizational, i.e., having to do with the necessity for bureaucratic reorientation in order to accommodate to the new technology, and socio-legal, i.e., having to do with explicit restrictions on data sharing or "confidentiality." Moreover, the clear thrust in research, particularly since 1974, has been in two directions; further adapting technology to existing organizational arrangements -- thus minimizing the disjuncture between present bureaucratic structure and the technical requirements of data

3 In these cases, it is not necessary to "program" a computer, but, simply to select among a set of options which have been established in advance. In effect, then, the user is actually throwing "switches" in a program which already exists; not creating a program from scratch. Cf., footnote 5, following.

processing, and detailed study of the ways in which computer-based technology can be most easily introduced into the work environment. These two areas of inquiry -- the first largely conducted by computer scientists and the latter by social scientists -- have explicitly come together in an interest in how data base management systems can be addressed through the use of "natural language."

This problem is clearly laid out in a now famous paper by E.F. Codd dealing with so-called "casual users," i.e., ones with a minimum of computer skills whose use of a system is episodic or irregular:

If we are to satisfy the needs of casual users of data bases, we must break through the barriers that presently prevent these users from freely employing their native languages (e.g., English) to specify what they want. In this paper we introduce an approach (already partially implemented) that permits a user to engage a relational data base system in a dialogue with the objective of attaining agreement between the user and the system as to the users' needs.

4

Codd goes on to describe a means whereby systems may be created such that no previous experience with their organization or design and no programming skills are necessary in order to extract the information they contain.

To fully grasp the broader implications of these developments for individual privacy, it is useful to review the history of computerized

4 Codd, E.F., "Seven Steps to Rendezvous with the Casual User," IBM Research Paper RJ 1333 (#20842), 1974.

data processing in general, and in particular, how this has affected the way in which personal records have been dealt with by governments and other large-scale organizations.

B. The Development of Computer Systems

Computer scientists conventionally draw a distinction between two aspects of the development of computer-based technology, the design of "hardware," i.e., mechanical devices for taking in (inputting), storing, retrieving and analyzing data, and the creation of "software," the sets of instructions (algorithms) which determine how these tasks are carried out.⁵ Both must be clearly understood in order to assess the present and future capabilities of computer-based systems for storage and retrieval of personal records.

In recent years, there has been a marked growth in both the "hardware" and "software" capabilities of computer systems. Initially, computers were simply used to improve the efficiency of repetitive clerical

5 A computer is an electronic device which performs numerical or logical operations by adding together, or subtracting, electrical currents. In most computers, this is done through the use of a series of two-state elements, originally thermionic valves and now transistors and other devices. The "code" in a computer of this kind is thus in "binary" (0, 1) form. A user who wishes to issue instructions to the computer must write these in one of several higher-order languages (e.g., FORTRAN, COBOL, APL) which are then interpreted by the computer and translated into sets of electronic operations. A consistent set of these instructions, in proper order, is called a "program."

operations (e.g., accounting, payroll, billing) which had previously been performed by electro-mechanical devices employing punch card input. Data had to be "coded" in advance (i.e., transcribed into numerical or alphabetic code), checked, corrected, and stored -- either in card form or on magnetic tape -- outside the machine except when they were being processed simultaneously ("batch" processing). The active workspace in most computers was extremely limited, and only one user could utilize a portion of the machine at any given time. Large jobs would, in effect, use up the machine for extended periods. Under these circumstances, there was virtually no change in the record-handling or data collection practices which had developed during the era of electro-mechanical devices.

In the early 1960's, the environment began to change. Larger machines and machine-systems greatly extended the amount of active core available to any given user, and improved speed greatly reduced processing time. Under these circumstances, large-scale organizations began to automate high-volume service activities, e.g., retail credit transactions, lists of customers, bank statements, insurance claims, and lists of motor vehicle drivers. Although this process is still going on, computerization of this kind had become extremely common by the end of the decade. The development of time-sharing (i.e., the sharing of active workspace by multiple users) allowed for much improved machine efficiency and made central data processing centres accessible from remote terminals. Improved media for data storage allowed for on-line processing of data

which could be called up by the user, automatically. These developments, in turn, both facilitated the use of computers as a locus for the actual storage (as opposed to processing) of data, and made it economical to use computers to retrieve relatively small amounts of information stored within much larger files. Software developments -- both the creation of powerful new languages (e.g., APL) for on-line use and improved text-handling capabilities -- kept pace.

By 1970, the stage was set for two important changes in the technological basis of computerized record-keeping. The first of these arose from the creation of multi-purpose software "shells," called data base management systems (DBMS), which were flexible enough to store apparently unrelated information for a variety of similar uses. The standardization of the software concepts involved led to the wide dissemination of commercially prepared DBMS packages. Coupled with earlier advances in hardware design, these systems greatly extended the forms of user access to stored data. For instance, data could be stored in "live files" and directly acted upon by users -- on-line query, on-line response; data could be queried on-line, but large data processing jobs (especially those involving large amounts of printing) could be undertaken later -- on-line query, off-line response; queries could be entered off-line, but results could be transferred to an active file; and queries could be entered off-line and responded to in a similar fashion. This increased flexibility greatly extended the potential use of computer systems for non-operational purposes such as management, planning and modelling.

The introduction and increased commercial availability of inexpensive data processing devices (e.g., silicon chips) led, in turn, to the creation of "intelligent" terminals⁶ which could be used to preprocess data directly from a remote data gathering device -- eliminating the need for extensive data encoding and checking since intelligent terminals could cull their own output. Improved data communications, further, allowed for the efficient transfer of electronically gathered data from remote terminals and their flexible storage and analysis, on-line, by a variety of users.

As a consequence, by the mid to late 1970's, it became technically feasible to: gather data, at source, electronically (e.g., enter transactions in a cash register); process these data locally using intelligent terminals or microcomputers; transmit these data to a central data processing centre; enter these data into a DBMS; and provide ready access -- to either random pieces of information (e.g., the name of a customer who bought a clock radio on a given day) or elaborate calculations done on these data (e.g., projected clock radio sales through the end of the year) -- to relatively unsophisticated users located at great geographical distances from one another, virtually instantaneously.

6 An intelligent terminal is a communications device which also has its own data processing capabilities. It is, in effect, a small computer.

The second change in computer technology with revolutionary implications for personal record-keeping has been the development, primarily during the last decade, of relatively inexpensive word processing devices and software systems. The proliferation of silicon chip storage devices has greatly reduced the cost of building systems for inputting, storing, and retrieving text form or natural language material. Together with concomitant advances in the ability of text processing languages to format documents, this development holds out the possibility that the vast majority of text form communications will be generated by electronic signal by the end of the decade. From the point of view of a low-level user, such systems have the advantage that a corrected (edited) draft can be printed directly, without the necessity for further correction or retyping. More sophisticated users can make use of them to: analyze and monitor outgoing communications; monitor the productivity of clerical staff; create multiple copies of form letters, where the content must vary by the characteristics of the recipient; and transfer natural language input into instructions for easy manipulation by a DBMS. In effect, given some sophisticated programming, it is entirely possible that, within a few years, the traditional line between "computerized" and "non-computerized" information will become almost completely blurred. Since the cost of such word processing systems is falling, and their capabilities increasing, it is quite likely that they will become accessible to even small organizations in the very near future.

Taken together, these two developments promise to revamp our information-processing and record-storing environment in the next decade. While the adoption of this new technology by Canadian governments has been relatively slow to date -- and a 1972 study by the federal Departments of Communications and Justice rejected the notion that invasions of informational privacy arising from computerization were either widespread or serious⁷ -- earlier technical and organizational impediments are likely to disappear or be greatly diminished in the near term. Moreover, restricted government budgets and rising wages for civil servants are likely to act as a further incentive for the introduction and intensive use of those technological capabilities which currently exist. Under these circumstances, the simple fact that violations of informational privacy do not seem to have been widespread in the recent past is no guarantee that they will not become so in the near future. Moreover, while technological forecasting is far from an exact science, it seems reasonably clear that, in the medium term, we can look forward to:

- a) an increase in the proportion of all communications generated in electronic form;
- b) an increase in the ability of computer systems to analyze as well as store and retrieve text from documents;
- c) an increase in the ease with which remote data systems may be linked together;
- d) an increasing gathering of transactional data by electronic means; and

7 Canada, Departments of Communications and Justice, Task Force on Computers and Privacy, Computers and Privacy (Ottawa: Queen's Printer, 1972) 182, 184.

- e) an increase in the extent to which these data may be accessed by even those with little or no formal training in computer use.

These trends suggest that a conscious effort is needed to ensure that informational privacy is maintained.

C. Security of Computerized Records

These continuing developments in the hardware and software capabilities of computer systems make it imperative that we seriously examine the issue of the security of computerized records. In general, we can distinguish between two related but separable problems:

- a) the security of these systems against penetration by "outsiders," i.e., those without authorized access to the system; and
- b) the security of these systems against unauthorized use of data by "insiders."

In this latter case, a further distinction needs to be drawn between such unauthorized use for personal gain, and for bureaucratic purposes.

Expert opinion has been consistent, over the last several years, in concluding that:

- a) no computer system is perfectly secure;
- b) time-share access to computer system greatly increases the likelihood that computer systems will be penetrated by outsiders;

- c) the greatest danger lies in the unauthorized use of data by insiders, not outsiders;
- d) storing data off-line limits access to it and, hence, unauthorized use; and
- e) restrictions on access to data are more likely, all things being equal, to increase security than restrictions on access to the machine itself.

Although no hard and fast distinction is possible in all cases, if we distinguish, for the moment, between machine security (i.e., the ability of a system to impede unauthorized access to its hardware) and file security (i.e., its ability to protect stored information) these issues will come into clearer focus. Machine security largely depends on the existence and patterns of use of the codes employed by users in gaining access to the computer system. The origins of these codes were in the necessity to account for and charge computer time to a given user, since early computer systems did not store data in direct access (completely automated) files, i.e., the user would store his/her data at some location remote from the place where actual data processing took place. Thus, their initial use was to prevent theft of computer funds, rather than enhance machine security.

Codes typically consist of two components: an account number, which identifies the user to the system and its personnel, and a lock or password which is the property of the user and whose dissemination is more restricted. Obviously, while unauthorized access to the machine by outsiders is impeded by the existence of account numbers and locks,

the former is of much more limited utility in protecting machine integrity against insiders. Codes are either numerical or a combination of numerical and alphabetical symbols. Since they are easier to remember, alphabetic character strings are usually used for locks.

Since an unauthorized user could gain access to a machine by simply generating random combinations of numbers and letters in the proper sequence until one such combination "hit," the real protection implicit in these codes lies in the large number of such combinations which one would need to try. In order to "break" a five-digit numerical code, for instance, one would have to try a very large number of possible combinations. If one combined this five-digit code with, say, a seven-letter lock, one's chances of breaking a code would become commensurately smaller.

On its face, then, illegally entering such a system would seem to be prohibitively time-consuming in the best of conditions. There are three reasons why this is not the case under certain circumstances. First, some systems permit users to generate information in one sub-system or a "foreign" system and marry new information to the original system. Under these circumstances, if the target system permits a user an unlimited number of "tries," it is possible to use one computer to generate combinations until one such number "hits." Second, given the increased availability of intelligent terminals, one may not even need a very sophisticated device to break the code in this fashion. Third,

users typically use meaningful alphabetic character strings for their locks -- and there are many fewer such strings than one would find by randomly combining letters. In fact, users often use their own first names (up to the limit provided by the allowable string length), their spouses names, their month of birth, and other similar character strings as locks. As this practice is a well-known phenomenon, programmers often gain access to one another's accounts by trying codes comprised of character strings of this kind.

For outsiders, these problems are simplified if one is interested in gaining access to any account within the system -- rather than a particular account -- since, if a system is heavily used, almost all numerical account codes will be assigned to someone. By choosing a given numerical code -- say 55555 -- one can reduce the problem to simply finding its corresponding alphabetic lock. Some systems, moreover, will feed back information to individuals entering the system which will provide hints as to how to break the code by indicating why a particular code is unsuitable, e.g., it will respond with the words "number not in system" rather than "improper password" when 55555 has not been assigned to a user.

In any event, if those wishing to penetrate a system are persistent enough, none of the barriers introduced by codes and locks are insuperable. Further, while increasing the number of symbols in a code or lock would exponentially increase the difficulty in illegally entering

a system, users are resistant to very long and cumbersome codes and locks since these impede legitimate access to the machine.

A more reliable way of increasing machine security is to control access to the machine by controlling the terminals through which it can be addressed. As a result, high security systems usually are "hardwired," i.e., directly connected to the machine by a dedicated line, rather than coupled through public telephone lines, in order to restrict their vulnerability to penetration. Once again, however, this method of control is far more effective in excluding outsiders from unauthorized access than insiders.

Although both hardware and software technology has been developed in recent years to increase machine security, there is a general recognition that the crux of the problem lies in file security and not in machine security, per se. Given that someone has successfully entered a machine, there are a number of impediments which may be placed in his/her way to maintain security of its records. In the limiting case, data which is not stored in the computer cannot be accessed through it. High security systems often do not allow for long-term direct access storage for this reason. Another impediment which may be introduced is to allow only specialized classes of users access to the machine's programming capabilities. Data base management systems frequently include protections of this kind. Hence, even if one is successful in illegally entering an account, one's ability to tamper with it is limited. Since classes

of accounts can be created, it is possible, in principle, to restrict access to data for which a given user has no authorized use.

There is obviously a tension, in these respects, between the purely technological changes in computing during the last decade -- which have tended to promote ease of access -- and the requirements of file security. As in most things in this area, there appear to be no easy answers. On-line data entry and processing is, for instance, more secure than batch processing in the sense that there are fewer intermediate forms of data created, e.g., coding sheets, punch cards, which need to be protected. By contrast, however, on-line systems are more easily penetrated in a systematic fashion than batch systems. Small stand-alone (dedicated) computers are, in most cases, easier to protect from outsiders than large systems. However, few small systems are sophisticated enough to foil a determined insider.

One technological development, which is still in its infancy, promises to greatly reduce some of these difficulties: distributed data bases. Under some designs for these systems, while access to some of the information stored in a series of remote locations is allowed, other classes of information are not shared. Thus, they involve some of the advantages of centralized data processing, but without some of the difficulties involved in protecting a large centralized system.

Even where one has been relatively successful in constructing technical barriers to unauthorized use, however, there are a number of ways in which insiders or outsiders can gain unauthorized access to confidential information. Given that the data being extracted from a machine is manipulable, it is quite possible for a user to gain access to bodies of information which do not, in themselves, disclose personal information or breach confidentiality, but which, taken together, may be used to do this. For example, let us assume that a government insider could gain legitimate access not only to the date of birth, sex, and occupations of persons in a given area of a city and to a detailed list of the billings by physicians located in that area, but also to the date of birth of those physicians and their specialties. Under many circumstances, it would be possible to create a unique cross-matching of these physicians, calculate their incomes by applying the appropriate weightings for billing purposes, and retrieve a list of patients for each of them. Examples of this kind militate in favour of highly centralized systems where the combined use of data files can be more effectively monitored. Under most circumstances, while it is relatively easy to establish procedures against the disclosure of information of this kind which will be successful in deterring their use for personal gain, it is not as easy to limit their use for bureaucratic purposes, i.e., monitoring of physicians, even where these have been deemed to be beyond the scope of government activity. In the final analysis, only the establishment of firm policies on disclosure of data, a carefully devised system of internal controls, and auditing of data usage will succeed in limiting incursions of this kind.

D. Technological Change and Privacy

The computer as a social artifact, then, has great potential for both good and ill. Under certain circumstances, as we noted earlier, computers can be used as tools for the protection of individual privacy by carefully monitoring access to and use of files.

Computer technology is, however, developing rapidly and it is difficult to forecast the directions in which it will turn. Nonetheless, a study undertaken for the Privacy Protection Study Commission attempts to give rough estimates of the likely future paths in its development and to indicate the significance of expected technological change for privacy protection issues.

The rate of change observed during the past 25 years is summarized in the PPSC report as follows:

- . Maximum processing speed has increased over 50,000-fold;
- . High-speed memory capacity has increased over 10,000-fold;
- . Reliability has increased over 1,000-fold;
- . Physical volume has been reduced over 100,000-fold; and
- . Cost per operation/price-performance has been reduced over 100,000-fold.

Computers that required hundreds of cubic feet of space 25 years ago have been supplanted by ones that take only a few cubic inches -- and operate a hundred-fold faster.

The PPSC report goes on to speculate that "further growth of at least 100-fold and perhaps 1,000-fold can be obtained from technology now known and understood."⁸

Predictions premised on "technology now known and understood" may, of course, be swept aside by the occurrence of as yet unforeseen technological "breakthroughs." If past history is any guide, it is not at all improbable that predictions such as those advanced by the PPSC will be shown to have been unduly conservative.

The most important point to be drawn from this is that in the very near future, cost is likely to disappear as a mechanism which may be used to create incentives for the preservation of privacy values. At the present time, pressures on information managers to maximize efficiency conduce to the reduction of privacy invasion. To the extent that the collection and storage of information creates significant cost, it will be a sound management policy to reduce data collection to the minimum necessary for the purposes in question and to destroy data whose storage costs exceed its value. Similarly, the conversion of manually-stored data to computer-stored data has proceeded at a less rapid pace than early observers have predicted, in part as a result of the cost of conversion. Although the spectre of widespread linkage of existing data bases has

8 United States Privacy Protection Study Commission, Personal Privacy in an Information Society, Appendix 5: Technology and Privacy (Washington, D.C.: USGPO, 1977) 14.

given rise to considerable anxiety, the expense involved in accurate linkage of personal data from one data bank to the next has, in some measure, restrained the integration of computer records holding personal data.

Privacy protection policy planning for the immediate future, however, must acknowledge the fact that cost disincentives of this kind are rapidly disappearing as a factor in information systems planning due, in large measure, to silicon chip technology,⁹ and that future developments along these lines are not unlikely.

Given this environment, then, no purely technological solution to the security and protection of privacy in record-keeping within computer systems is likely to be effective in the long term.

E. Automation of Personal Records
in the Ontario Government

Our review of the personal records systems maintained by the Ontario government indicates that automation has taken place in the traditional manner, and that most systems are, in fact, simply automated versions

9 Through the use of recently developed micro-electronic manufacturing technology, a single silicon chip, typically one-quarter inch square, can be impressed with the circuitry and memory banks necessary to constitute a complete "micro computer." See ibid., 65.

of the pre-existing manual records — with little change in either the form or content of the stored data. In all the cases we examined, some sort of manual system remains in place to provide a "hard" (non-electronic) record of the original or "source" document. In some instances, documents are microfilmed to reduce storage costs and the originals are then destroyed. The effect of computerization is not, therefore, to increase the amount of data collected and maintained on file, but to allow these data to be more rapidly and intensively utilized.

Most of the information collected by Ontario government agencies is used in the direct day-to-day administration of the various programs for which they are responsible. However, computerization can greatly facilitate the compiling of statistics and the production of reports. In some instances, this has been a deciding factor in moving a given ministry in the direction of automated storage and retrieval of its records. Moreover, although the ability to rapidly analyze data can encourage increased data collection, we observed that the cost associated with increased data gathering and processing has proved to be an effective barrier, under present circumstances, to the development of computer systems solely for planning purposes. Thus, the thrust of program management within Ontario government agencies has been towards improving the operational efficiency and effectiveness of their systems, and not towards the proliferation of new data management activities.

No central data bases have been created to which multiple users with distinct administrative functions in different ministries have access. There is, however, cross-sharing of information amongst different ministries and agencies -- some of this via remote terminals. For example, motor vehicle files in the Ministry of Transportation and Communications can be directly queried by police through a mini-computer linked to a provincial communications network and to the Canadian Police Information Centre in Ottawa. However, queries can only be sent in one direction: Ministry of Transportation and Communications personnel cannot access police records. This is, of course, a legitimate use of vehicle records, but it also serves as an example of how communication systems can provide some of the efficiency associated with a central data base while allowing specific agencies to preserve control over their records. Thus, in this particular instance, there was no need to amalgamate files.

In 1976, a special task force appointed by Management Board of Cabinet identified 117 government-operated data systems in Ontario which contain personal information. Of these, 14 are in the planning stage, 13 are under development, and 90 are implemented and/or fully operational. Of the 117 Ontario government systems, 83% are (or will be) housed in one of three government computer centres. An additional 10 such systems are implemented on ministry-owned mini-computers, and nine are operated through private service bureaus. The Ontario government's data centres are operated by the Computer Services Division, Ministry of Government

Services, which:

provides computer services in support of the operational programs and service-delivery functions of ministries and agencies of the Ontario government.

10

The Division consists of three separate computing centres, located in the Toronto area, and the Computer Support Services Branch. Each of the computing centres is predominantly used for operational or administrative data processing. However, each centre, to some extent, performs a full range of data processing functions.

Downsview Computer Centre: is predominantly concerned with supporting continuous access to data base management systems (DBMS) via a province-wide telecommunications net. This centre also supports engineering and scientific applications. Its hardware includes IBM/158 and IBM/168 processors. Major users include the Ontario Ministries of Transportation and Communications, Environment, Revenue, the Ministry of the Solicitor General, and Consumer and Commercial Relations.

Leaside Computing Centre: is predominantly concerned with supplying very large regularly scheduled batch processing. An example of this would be the kinds of services regularly required by the Ministry of Health. This centre is also where new technologies are tested in an

10 Ontario Ministry of Government Services, Annual Report for Fiscal Year ending March 31, 1977 (Toronto: Ministry of Government Services, 1978) 18.

operational environment prior to widespread adoption by the Division. The main processor at Leaside is an AMDAHL 470 V/6-11.

Queen's Park Computing Centre: is principally concerned with supporting unscheduled batch processing -- both over-the-counter and via remote terminal access. The computer processor used at Queen's Park is an IBM 370/168-AP. The system provides services for over 100 accounts -- including those held by the Ministries of Education, Government Services, Revenue, Community and Social Services, and the Attorney-General.

Computer Services Branch: plans new development and supplies specialized services to other parts of the Division.

The Division as a whole operates on a full-cost recovery basis in competition with private service bureaus.

The 1976 special task force report to the Management Board of Cabinet examined the adequacy of privacy protection and security in the information practices of the Ministries of: Health, Consumer and Commercial Relations, Colleges and Universities, Education, Solicitor-General, Revenue, Transportation and Communications, Labour, and Community and Social Services. The task group examined publications of these ministries, conducted questionnaire-based research, interviewed personnel, and performed on-site inspections. In addition, they studied the measures undertaken to protect privacy and provide security elsewhere. The study

concluded that, while there was little evidence of information privacy violations, the potential for violations of both machine security and file security was "large and growing." For the purposes we are concerned with here, while the task group reported that the responses to its questionnaires indicated that such security was, in general, reasonably good, it did note serious difficulties in the machine security arrangements (protection of lines, control codes, etc.) and data handling practices at one centre and in the operating practices of another.¹¹

In 1978, Management Board commissioned a further study which, among other issues, examined the security of one data centre in detail. The consultants who carried out the study concluded that physical security and systems control in the data centre were adequate.¹² Each data centre has an officer who is specifically concerned with security, and the Computer Services Division also has a security officer who advises client ministries on security matters.

The need for security in individual ministry data preparation areas is indicated by the fact that over half of the systems allowed for remote

- 11 Ontario, Privacy Project Task Force: Report and Recommendations, Ontario Management Board of Cabinet (Toronto: July, 1976) 8-12; Appendix A: Privacy and Security Survey on Information and Individuals, Management Consulting Services Division, Ministry of Government Services (August, 1975).
- 12 Ontario, Management Board of Cabinet, Confidential Security Audit, 1978. The research staff was not permitted to review the audit report itself, but was permitted to take notes at a meeting discussing its findings.

terminal data entry, although the systems integrity study again commented that security procedures for originating transactions, data entry, data communications and computer processing for the eight systems examined were generally adequate. There are, however, no overall standards for systems security within the Ontario government beyond those stated in the Manual of Administration (Table 1).

Although many Ontario government personnel data files pass through or are stored in one or other of the three large data centres, this does not mean that these data are, necessarily, being cross-shared or amalgamated into one file. Information may be processed or stored in a data centre but the data systems, their operations and their storage, kept totally separate. Data centres typically have elaborate provisions to ensure that only authorized processing or data transfer occurs -- not only between offices, but within them. In fact, in any good multiple-use computer facility, the users are segregated and, as a rule, unaware of each other's presence on the system. We are not in a position to fully assess these issues here -- since we could not conduct an inventory of these security measures on our own. The consultants report to Management Board deems that the measures employed by these centres are adequate at the present time. We are unable, however, to establish this independently.

TABLE IV.1

ONTARIO MANUAL OF ADMINISTRATION
SECTION 55.2.5

Security of Systems

In order to ensure that operational systems and master files are secure from destruction because of errors and acts of vandalism or nature, the following minimum standard practices shall be followed:

1. Primary responsibility for the security of master files and data shall rest with the user.
2. All programs shall have up-to-date duplicates, and master files shall have back-up data in a form so that up-to-date master files may be easily and quickly recreated.
3. One complete set of up-to-date source programs and back-up data in a form so that up-to-date master files may be easily recreated shall be kept in a building other than the one where operating programs and files are processed. This off-site storage shall be in a secure and restricted area under government control.
4. Procedures shall be developed for the transfer and storage of data for each system dealing with confidential data. These procedures shall be approved by the responsible Branch Director or the responsible Division Executive Director. Also, in the case of systems with financial implications, the responsible financial officer shall approve the procedures.
5. Data processing centres shall develop procedures dealing with security of the facilities of the data centre, including restrictions on movement of personnel in the data centre.
6. Records retention arrangements shall reflect the requirements of the Vital Records Guidelines issued by Management Board.

F. Privacy and Computers

We have seen that, while the nightmare of an environment in which every significant act or transaction of a citizen is open to government scrutiny has not materialized, important technological barriers to the creation of such an environment have been or are being eliminated. Moreover, given recent software developments which have had the effect of adjusting computer systems to bureaucratic practice -- rather than vice versa -- significant organizational barriers to the introduction of new computer technology have been lowered as well. The impact of these changes -- together with the possibility, within a decade of the almost exclusive use of computerized word processing systems for the generation of written communications -- has been to make it imperative that we seriously consider socio-legal constraints on computer use which may be effective in reducing the possibility that abuses of privacy will occur.

At the moment, there is no evidence that data processing or personal record-keeping by the Ontario government is such that deliberate or systematic misuse of files by the Ontario government is going on. There is little sharing of data between agencies via computer links and no large integrated data banks have been created. On the basis of the information we have at present -- but recognizing that we were not able to examine this issue directly -- it appears that both machine security and file security, while not perfect, are adequate for the short term.

However, it must be stressed that no computerized record system is absolutely secure and any system, given the will and the resources, can be penetrated. Moreover, even if record systems and hardware currently in use were perfectly secure given present technology, new technological developments could render current security arrangements obsolete rather quickly.

Both the Ministry of Health and the Ministry of Community and Social Services are considering moving towards large integrated data base systems, which would include data drawn from a number of different programs. This obviously increases the sensitivity of their record systems in that each individual's personal record will contain more information which will become, in turn, more accessible to ministry personnel. Developments such as these highlight the need for a continual review of procedural and machine security standards by a professional task group without operational responsibilities for the direct day-to-day administration of government record-keeping systems. Subjective data, such as those stored in computerized intelligence systems, should be especially carefully scrutinized.

CHAPTER V

PERSONAL IDENTIFIERS: THE DEVELOPMENT OF A SINGLE IDENTIFYING NUMBER

Various terms are used to describe the different ways in which people may be identified when information about them is recorded. These "identifiers" have traditionally served three purposes within record systems. First, they identify each individual's record, separating it from others. Second, they provide one easy means of locating an individual record in order to update it or to use it for administrative purposes. Third, they may be employed in indexing personal records in some logical fashion,

Terms describing these identifiers arising in our discussion are:

- . Unique Personal Identifiers (UPI): numbers, letters or symbols, unique to each individual whose record is contained in a system.
- . "Standard Identifiers": standard because they are the pieces of information by which personal records are conventionally identified; such as name, address and age. An example of their use is the alphabetical filing of a record index by name.
- . Single identifying number: a single number which identifies a person in all record systems where information about him/her is stored. Bestowed on all members of a population at birth or when they migrate into a country, the number is usually referred to as a "personal registration number," or "universal personal identifier."

- . Social Insurance Number (SIN): perhaps the best known identifier in Canada. The nine-digit Social Insurance Number, widely used since its inception in 1964 under the Canada Pension Plan Act, is not yet a single identifying number. As we shall see, its potential for adoption as the identifying number of all Canadian residents has increased in recent years.

Given this brief set of definitions, let us now turn to a discussion of unique personal identifiers and single identifying numbers.

A. The Change from "Standard Identifiers"
to Unique Personal Identifiers

The assignment of Unique Personal Identifiers to individuals, accounts, situations or cases is a natural outgrowth of the increase in record-keeping by large organizations. "Standard identifiers" have always been used in large record systems. As more records are kept, and for longer periods of time, "standard identifiers," some of which are not held constant over time, are increasingly inadequate for a quick, one-step search. The use of such identifiers often yields a number of possible records which must be winnowed, using other information in order to locate the correct one. For example, all "Smiths" in a file would have to be searched using some other characteristic in order to find a particular "Smith." Depending on the precision of an identifier and the time lag between data entries (some identifiers, such as address, change frequently), the "hit-rate" (the number of initial positive confirmed identifications not requiring further checking) can

vary tremendously. In many systems, further checking can be costly and time-consuming.

There are two principal purposes served by UPIs. They assist in establishing that a person with a given "standard identifier" is in fact the correct person. The desire for unchanging, Unique Personal Identifiers is, therefore, understandable. This trend has a long history, as exemplified by the use of such devices as employee numbers, case numbers and account or loan numbers. However, the computerization of records served to reinforce the argument for unique identification: the need to eliminate cross-checking or manual verification in order to improve search efficiency.

Second, from the point of view of privacy protection, UPIs have distinct advantages over other types of identifiers. Because an individual is less likely to be confused with another, s/he is unlikely to be blamed for a misdeed of another, or pursued by a government agency seeking another person with a similar name or address. Unique Personal Identifiers may be designed to be unique also to a system, meaning that an individual's record in one system is unlikely to be matched with his/her record in another system. This type of UPI allows an individual to retain a degree of anonymity as s/he comes into contact with various government agencies throughout his/her life. The privacy protective ability of a UPI is further improved if the identifier chosen is meaningless in itself, that is, if it bears no

relationship to any client characteristic, date or program characteristic.

However, when the same Unique Personal Identifier comes to be used by several separate agencies with different objectives, the problems of data linkage and potential loss of record subject privacy arise. The Unique Personal Identifier, used internally by an organization, then begins to become a much more sinister vehicle for information transfer -- the single identification number.

B. Single Identifying Numbers

The chief advantages of a single identifying number over other means of record identification is that it can be used to facilitate record linkage. In the same way that Unique Personal Identifiers in a system permit better record identification for the accessing of records, a universal single identifying number permits more efficient "interface" of personal data systems. This "interface" promotes greater accessibility to personal information systems, and in effect creates a single system by making possible the merging of information in several different systems, without physically moving the data banks together.

The benefits accruing from this are many: the increased information base available (from merged data systems) for government program

decision-making; a decreased amount of duplication in information gathering; and an expanded information base for statistical purposes, in research, planning and administration.

There are also two potential benefits to the individual about whom records are being maintained: the benefits of more accurate record-keeping; and the ease of dealing with just one organization, instead of many, to access personal records, provide information for correction or updating, or to track and control record dissemination. However, it must be realized that such benefits can only accrue to the individual if systems are designed to provide them. The majority of data systems examined in the course of our research provide none of these benefits to record subjects. Thus far, proposals for single identifying numbers to be used by government have been based on improved administrative efficiency, rather than on any direct benefit to the individual.

There are two basic positions against the use of a single identifying number. The first argues that the use of numbers is a further "dehumanizing" influence on our already overly bureaucratized government administration, and indeed on all large, seemingly faceless organizations.

The second argues that use of such numbers will facilitate further invasions of privacy or intrusions into private lives because of an enhanced ability to link data bases into what effectively would be a national data bank of dossiers on every resident without record subject

permission or knowledge.¹

As far as the first position is concerned, it seems to us that the single identifying number issue is simply one of many aspects of the problem of remoteness in our institutions, and that in fact it might not be one of the more important ones. If large organizations were more approachable, flexible and open in their dealings with the public, then perhaps the single identifying number would not be seen as such a threat to human dignity, but rather as a neutral tool of administrative technology. Such considerations are part of a deeper debate than is possible within the context of this report.

The second position raises the issue of the potential for privacy invasion which might arise from the use of a single identifying number. The linkage of different record systems and the exchange and consolidation of information about people may not always be beneficial to the individuals concerned. Such linkage, exchange and consolidation of information is, of course, quite possible without a single identifying number.² Also stemming from this fear is the misgiving

1 According to Arthur Miller, Assault on Privacy (Ann Arbor: University of Michigan Press, 1971), it was this fear which aroused public fervor against a U.S. centralized collection of personal record systems to be indexed by Social Security Number.

2 The method for identifying individuals by using a combination of standard identifiers or "natural" variables, such as age, sex, income and profession, where unique identifiers are not recorded, is called "Backwards Identification." For an explanation of the

(cont'd)

that newly created government-held dossiers will follow people throughout their lives, and that, in the case of wrong-doing by the individual, will not allow him/her to "make a fresh start."³ The threat of social control resulting from the creation of such dossiers is obvious.

Both these positions against the use of single identifying numbers originate from a justifiable concern for privacy protection if data which has been collected in one context for one purpose is used in an entirely different context and for a different purpose. The risk of what is known as "non-derivative use" of personal information may be heightened by the enhanced ease of data sharing through a single identifying number. However, the "non-derivative use" problem would not be resolved merely by banning single identification numbers. Rather, its resolution requires data protection rules which prohibit certain types of record transfers for unconnected purposes, and which require subject authorization prior to any record transfers from the original source of record collection.

- 2 (cont'd) computer techniques utilized in backwards identification and their statistical probability of success, see Olsson, Lars, Backwards Identification (Sweden: National Central Bureau of Statistics, 1975).
- 3 Conversely, reliance on single identifying numbers for identification purposes can enhance an individual's ability to "make a fresh start." For example, to disguise the identity of a former undercover agent, a security service agency may arrange for the agent to be given a new number, effectively separating him/her from a nefarious past.

Our overall impression of the controversy over use of single identifying numbers is that it is just one component of the issue of data protection. As we have said, data identification is already quite sophisticated in the absence of single identifying numbers and data linkage may be satisfactorily accomplished without their use.

C. Personal Identifiers in
the Ontario Government

Ontario government programs use a wide variety of identifiers to identify and authenticate individuals and records: "standard identifiers" such as name, address or birthdate; specific application identifying numbers (Unique Personal Identifiers) such as driver's licence number, vehicle licence number, birth identification number, etc.; case numbers (also Unique Personal Identifiers) such as those used in social services and certain health programs; and more widely recognized UPI numbers such as OHIP number and the Social Insurance Number (SIN).

It was our observation that in the majority of record systems, more than one identifier is collected, even if they are not all used for record retrieval purposes. In such systems, records are often filed by name, but a number (such as a case number) serves to verify that every record added to the file applies to the correct person. In large record systems, and particularly those which are automated, records are filed by both name and a Unique Personal Identifier. For example,

in the computerized government employee information system, records are filed by both name and Social Insurance Number, and in the driver licensing system, by both name and driver licence number. With the flexibility of data base technology, it is of course possible to store and retrieve individual records by any of a variety of identifiers.

Particularly in large computerized systems, use of more than one identifier is an important protection to the individual, ensuring that the correct record about him/her is used and not someone else's record. This protection is the reason why the most extensive range of identifiers is collected by law enforcement and corrections agencies. In addition to physical description, these agencies collect driver licence number, Social Insurance Number and fingerprint identification number.

One exception to this use of Unique Personal Identifiers for verification purposes is the Personal Property Security Registration System, which, although it is very large and volatile, identifies only by name and address. The policy of not using unique identifiers has led to some criticisms, because general inquiries of a name can yield a long list of record entries (e.g., all the John Smiths on the system), which some claim to be an invasion of the privacy of the wrong John Smiths.

The two most common numbers collected, as indicated by the Ontario

Privacy Task Group in 1976,⁴ and confirmed by our own studies, are the Social Insurance Number (SIN) and the OHIP number. This latter number is, of course, used primarily in health or medical areas, but social assistance providers and subscribers to OHIP, such as government employers, also record the OHIP number to facilitate linkage with the health insurance system.

D. The Growing Use of the Social Insurance Number
as a Single Identifying Number

Social Insurance Numbers were originally intended for use in administering the federal unemployment insurance scheme instituted in 1936. Their adoption for use in tax collection and pension disbursement under the Canada Pension Plan was not accepted by Parliament until 1965⁵ after a year of heated debates. At the time, the required use of numbered identification cards was construed by some members of Parliament as an invasion of individual privacy; with overtones of social control. As early as April, 1964, the Right Hon. J.G. Diefenbaker, Leader of the Opposition, expressed some of these concerns to the Hon. Mr. MacEachen, then Minister of Labour:

4 Ontario, Privacy Project Task Force: Report and Recommendations, Ontario Management Board of Cabinet (Toronto: July, 1976) 24.

5 Canada Pension Plan Act, S.C. 1965, c. C-5, s. 100. The original Social Insurance Number registration system actually came into effect one year earlier, under Regulations of the Unemployment Insurance Act, R.S.C. 1955.

I would also like to ask him whether he would give the assurance to the Canadian people — and it does not appear in the application — that any information provided in this application form will be maintained on a completely confidential basis and will not be used for any other purpose or passed over to any other department?

Mr. MacEachen's answer provided a portent of what would become a serious privacy issue in the late 1970's:

My honourable friend will recall that the Glassco Commission made a proposal that there be a common system of government record-keeping and I am saying ... that this information is to be used for the unemployment insurance system and for the Canada Pension Plan ... I am not in a position to indicate at this stage what system of government record-keeping will be involved in the future, but that is the present attitude of the government.

6

Under pressure not only from members of the Opposition, but also from various unions and the general public, the Pearson government included a section in the Canada Pension Plan Act which specifically assures individual contributors and beneficiaries that personal information communicated to personnel administering the Act will be considered "privileged," i.e., not to be revealed to anyone except employees in five specified departments "where it is necessary to do so for the purpose of the administration of this Act."⁷ In the words of the Minister of the Department of National Health and Welfare, this

6 Canada, House of Commons Debates (1964 Session, April 8, 1964) 1917. Mr. Diefenbaker added that the system seemed to "bear a strange relationship to dictatorship."

7 Canada Pension Plan Act, S.C. 1965, c. 51, s. 107. The bodies authorized to exchange such information were the Department of National Health and Welfare, the Department of National Revenue, the Department of Finance, the Unemployment Insurance Commission and the Dominion Bureau of Statistics.

stipulation and associated penalties for its violation

... should indicate to all honourable members the importance attached by all departments and by the draftsmen to the necessity for keeping the information secret, for keeping it confined to the department which receives it, except for the purposes of this Act.

8

Since 1964, amendments to section 107 have extended the list of departments and other bodies allowed to exchange social insurance information. These changes have altered the original guarantee that all such exchanges will be used solely for the administration of the Canada Pension Plan Act,⁹ in that the Employment and Immigration Commission may now utilize SIN information to administer the Unemployment Insurance Act of 1971, and provinces may now use federally collected SIN information to administer and enforce health insurance legislation.¹⁰

Although it has periodically been expanded, the specific list of departments and agencies authorized to receive SINs under the Canadian Pension Plan Act is considered potentially more useful in protecting privacy than two "confidentiality sections" of the Unemployment Insurance Act. The first of these gives the Minister of Employment and Immigration discretionary powers to release information obtained by the Unemployment Insurance Commission or the Department of Employment and

8 Canada, House of Commons Debates (1964-65 Session, March 2, 1965) 11898.

9 Canada Pension Plan Act, R.S.C. 1970, c. C-5, s. 107(3) (e.1) (4), as amended by R.S.C. 1970 (2nd Supp.) c. 33, s. 1.

10 Canada Pension Plan Regulations, P.C. 66-580, s. 802.

Immigration (including Social Insurance Number) "to such other persons as the Minister deems advisable" The second permits the Unemployment Insurance Commission to make Social Insurance Number information available "for the accurate identification of individuals ... to such persons as the Commission thinks appropriate to accomplish such purpose."¹¹

Despite statutory directives and assurances of confidentiality, use of SINs for purposes quite different from those stated in either Act is becoming common, in both federal and provincial government record systems.

Most provincial health, education, personnel, law enforcement, corrections and social services programs use it in establishing their personal record files.¹² In many cases, the number is required for tax or payroll purposes. In others, it appears to have been collected precisely because of its anticipated use as a universal single identifying number in the near future. In fact, we were told by many government interviewees that space for a nine-digit number had been provided on collection forms in the expectation that a universal number

11 Unemployment Insurance Act, S.C. 1971, c. 48, s. 114, as amended by S.C. 1977, c. 54, s. 60.1. The second provision is contained in S.C. 1971, c. 48, s. 126(4).

12 Elsewhere in this report, we examine, in detail, proposals for the use of Social Insurance Numbers as identifiers in Ontario income maintenance systems (Chapter VIII) and health care systems (Chapter XI).

would be adopted at some point. Many administrators believed that a single identifying number such as the Social Insurance Number would be desirable for efficient administration of programs.

This expanded use of Social Insurance Numbers by Ontario programs has been actively encouraged by the federal government. Federal departments and agencies utilizing SIN to index personal data systems include the RCMP, CIDA, Defence, Agriculture, Fisheries, Consumer Affairs, External Affairs, Health and Welfare, Indian and Northern Affairs and the Post Office. One indication that federal agencies have, de facto, adopted the SIN as a single identifying number is the requirement that individuals use the number in gaining access to their personal files in the majority of data banks listed under the Canadian Human Rights Act, Part IV.¹³ Another indication of this trend is the replacement of Regimental Service Numbers with Social Insurance Numbers in the Canadian Forces record systems. Recently, in letters sent to parents of public school pupils,¹⁴ the Canada Employment and Immigration Commission encouraged early acquisition of Social Insurance Numbers. In October, 1978, National Health and Welfare Minister Monique Begin commented thus:

13 Canada Treasury Board, Index of Federal Information Banks: 1979 (Ottawa: Minister of Supply and Services Canada, 1979), and Government of Canada, Record Access Request Form (Canadian Human Rights Act, Part IV) form no. TB/CT 350-9(12/77).

14 Letter to the Commission on Freedom of Information and Individual Privacy, December 20, 1978 containing copy of Employment and Immigration Canada letter to all public school parents in Frontenac, Lennox and Addington counties, dated February 14, 1978.

Canadians should expect their Social Insurance Numbers to be more widely used as identification in the computer banks of government and private industry ... [This is] a policy of common sense ...

15

In such an atmosphere, the acceptance of SINs as universal single identifying numbers could become a self-fulfilling prophecy.

Large-scale governmental use of the number has not been limited to publicly known programs. Briefs presented to the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, state that the RCMP has had unlimited on-line access to the central Social Insurance Number Index (which has registered more than 20 million people) since the start of the Unemployment Insurance Program. Moreover, it has extensively used personal information (e.g., location, relatives' names and employment history) contained in the Index and on file in regional offices of the Unemployment Insurance Commission, to identify and track down suspects.¹⁶ Testimony before the Commission also revealed that "the RCMP, apparently without the knowledge (or authorization) of unemployment insurance officials, processed requests from many other police departments [using information contained in the

- 15 Mann, Edward and John Alan Lee, RCMP v. The People (Don Mills, Ont: General Publishing Co. Ltd., 1979) 169-170, quoting The Globe and Mail, October 28, 1978.
- 16 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Mr. Justice David C. McDonald, Chairman, Hearings (Ottawa: The Commission, testimony beginning June 20, 1978) Vol. 57 and 58.

Social Insurance Number Index]."¹⁷

The widespread adoption of the SIN has not escaped public attention or been accomplished without opposition. Mr. Paul Shaver, for example, fought and won a battle with his daughter's local school board and her university over their required registration of pupils by Social Insurance Number.¹⁸ A similar protest against a Canada Employment and Immigration Commission letter encouraging early pupil acquisition of Social Insurance Numbers for use in "organized sports and activities such as hockey, baseball, Air Cadets of Canada and Sea Cadets of Canada," was voiced by a group of Frontenac County parents.¹⁹ In another recent dispute over use of the number, Ontario gun owners won the right to refuse to include their Social Insurance Numbers on applications for Firearms Acquisition Certificates. The Consumer's Association of Canada presented to former Revenue Minister Walter Baker a resolution against proliferation of Social Insurance Numbers for a number of illegal purposes.²⁰ The media have also been critical of

17 Sallot, Jeff, "How the Mounties got a direct line to your SIN file," The Globe and Mail, September 20, 1978.

18 Shaver, Paul, letter to Commission on Freedom of Information and Individual Privacy, January 10, 1979; and "Social insurance numbers are possible invasion of privacy, some fear," The Globe and Mail, September 19, 1978.

19 Letter to Commission on Freedom of Information and Individual Privacy, supra note 14.

20 "Ottawa has promised action on CAC complaint about SINs," The Globe and Mail, December 6, 1979.

the increasing governmental use of the Social Insurance Number to index police records, public health records, sensitive Manpower files, and to register babies at birth in Prince Edward Island.²¹ The media found especially objectionable a government proposal to identify and monitor foreign workers through specially designated Social Insurance Numbers.

Private sector use of Social Insurance Numbers is also increasing. It is now common to require people to present their Social Insurance cards to cash or write cheques,²³ buy or sell savings bonds, deposit and withdraw money in Registered Home Ownership and Registered Retirement Savings Plans, open bank and credit card accounts, receive private hospital treatments,²⁴ and reserve airline seats on chartered flights.²⁵ One of the most controversial private sector uses of the number is to identify workers on employee badges. Canadian General Electric recently provoked a union outcry against the

21 Sallot, Jeff, "Even babies get SIN as clever idea grows and grows," The Globe and Mail, September 19, 1978.

22 "Our number is up," The Globe and Mail, May 20, 1978.

23 For example, the Hudson's Bay Company specifically requests Social Insurance Number cards from cheque-writing customers in Ontario. The number is compared to a computerized system list of bad cheque-writers filed and indexed by Social Insurance Number.

24 Private hospitals in the Toronto area, for example, collect Social Insurance Numbers from all prospective patients and send records indexed by the number to a computer firm in the United States for regular statistical compilation.

25 Romain, Ken, "Mandatory SIN bothers air charter industry," The Globe and Mail, December 14, 1978.

practice.²⁶ Inger Hansen, federal Privacy Commissioner for the Canadian Human Rights Act, Part IV, has received numerous inquiries about use of SINs. The overwhelming majority of them were complaints about collection of the number by businesses -- particularly banks, insurance companies and employers. At present, the Commissioner has no powers under the Act to investigate or resolve such complaints.²⁷

Given the aforementioned examples, we may more closely define the threat to individual privacy posed by the widespread use of SINs as a single identifying number. First, the number is easily accessible. Most people carry Social Insurance Number cards with them. If such a card were stolen or lost, the thief (or finder) could then use it to discover a great many characteristics of the number holder from record collections which index personal information by SIN. If there were adequate technical and legal safeguards against penetration of these data banks, use of the number to find personal information about others would be extremely difficult and expensive. However, our research has shown that in many cases, the Ontario government's personal record collections and data banks are not adequately protected from such penetration and/or potential misuse.

26 "Union seeks to block use of worker's SIN on CGE plant badge," The Globe and Mail, December 12, 1978.

27 Telephone interview with Inger Hansen, federal Privacy Commissioner, November 6, 1979.

Second, the SIN is now the primary means of indexing enough data systems to enable someone to effectively link personal information in many record collections in both public and private sectors. Consumer profiles assembled with the aid of the number from information contained in Ontario government data banks might be attractive to marketers, bill collectors, insurance agencies, police intelligence agencies, private intelligence agencies and criminal elements.²⁸ It is possible, using other techniques, to assemble profiles from many different government data sources, or from government and private sector held data sources, without utilizing the Social Insurance Number, but at considerable time and expense to the unauthorized accessor. The large-scale use of the number as an indexer has made the profiling task much simpler, quicker and less expensive.

Third, provision of the number to government authorities as well as to commercial establishments is usually involuntary. Clients of both government and private services are usually not informed of the essentially optional need for their Social Insurance Numbers. Those who refuse to reveal Social Insurance Numbers are instead often denied service. In actual fact, as successful protests on the part of

28 For example, by combining data from several different, seemingly unrelated data banks such as census statistical tables, Motor Vehicle lists, and magazine subscriber lists, mailing list compilers may formulate "inferred variables" about potential customers for extremely refined marketing purposes. For a detailed discussion of the privacy-invasive possibilities of such linkages, see U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society (Washington, D.C.: USGPO, 1977) 127-141.

concerned citizens illustrate, the number is often not necessary to establish identity, retrieve files or gain access to service. Where a unique identifier is needed to call a particular record in a system, any identifier (for example, a nine-digit number contrived by the client or the service provider) will often serve the same purpose. Lack of Social Insurance Number or any other number should only slightly inhibit the locator abilities of sophisticated systems, most of which can be designed to call files by any or a combination of several identifiers.

The fourth aspect of the threat to individual privacy posed by large-scale adoption of the Social Insurance Number (or an equivalent Unique Personal Identifier), and perhaps the most important, is its use by the police. Without the awareness or authorization of unemployment insurance contributors (most employed people in the province), police have been accessing Social Insurance Number master files and other files capable of being located by the number over the course of many years. If these files, guaranteed to be confidential under the law, have been opened to police, citizens concerned about privacy may justifiably wonder what other personal files indexed by the Social Insurance Number have been or will be seen by police.

These four characteristics of Social Insurance Numbers, combined with the failure of many record systems to provide adequate safeguards against unauthorized users, appear to compose a valid threat to the informational privacy of individuals in Ontario.

E. Solutions

The expanded use of single identifying numbers has enhanced the need for a resolution of the conflict between the information and efficiency needs of government, and the privacy needs of individuals. Without specified information confidentiality safeguards:

... there can be no assurance that the consequences for individuals of such linkage and accessibility will be benign. At best, individuals may be frustrated and annoyed by unwarranted exchanges of information about them. At worst, they may be threatened with denial of status and benefits without due process ...

29

The key to the issue, then, is the provision of safeguards against unauthorized linkages or transfer of data, whether or not single identifying numbers exist. In its 1978 report, the Swedish Committee on Data Legislation (DALK) did not recommend any prohibition or extensive restriction on the use of identity numbers in personal registers in that country, preferring instead to recommend that "attention should be paid to how data are made available and to whom." The Committee concluded that:

... the elimination of identity numbers in personal registers would place no decisive obstacle in the way of linking of registers ... Methods for such purposes exist and are already in use ... The elimination of identity numbers would, however, have extensive consequences without attaining the desired result. DALK would particularly emphasize in this context the high costs, which cannot be definitely established without

29 U.S. Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens (Boston: Massachusetts Institute of Technology, 1973) 121.

thorough investigations but, to some extent at least, must affect the individual in the form of higher charges and prices.

30

Although safeguards for data, as opposed to controls on identifiers, have been emphasized by some governments, proposals to employ single identifying numbers for all types of personal data stored in government data banks, necessitating registration of the entire population, have occasionally encountered stiff public resistance. In the Netherlands, for example, opposition to such a system was traced to recent experiences under a totalitarian regime:

During World War II, a perfect system of population records combined with personal identity cards had facilitated the arrest and deportation of thousands of innocent people by the German occupation forces.

31

Many jurisdictions have seen fit to limit use of single identifying numbers by law. Both Norway and France have empowered data protection authorities to regulate the use of personal identification numbers.³² Under the French Act, permission of a legislative body, the Conseil d'Etat, as well as the National Committee on Data Processing and Freedom, must be obtained in order to use the national index

30 Delbetankande av datalagstiftningskommitten (DALK), Personregister -- Datarer Integritet, Summary (Stockholm: DALK, 1978) 344-345.

31 Hondius, Frits, Emerging Data Protection in Europe (New York: American Elsevier, 1975) 41.

32 Report of the Committee on Data Protection, (Lindop Committee) (Cmd. 7341, 1978) 261-262.

identifying persons (similar to the Canadian federal SIN index) for any type of personal data processing.³³ In its revised Data Protection Act, Germany has abandoned altogether the introduction of a planned SUI (Standard Universal Identifier).³⁴ The Lindop Committee on Data Protection has recommended that Great Britain assign an independent Data Protection Authority the responsibility of restricting, in codes of practice having the force of law, the collection and uses of any personal identifier intended for any private or public sector personal information system.³⁵

In the United States, the federal Privacy Act imposed a moratorium on collection of an individual's Social Security Number (that country's equivalent to the Social Insurance Number) by government agencies.³⁶ Although the Privacy Protection Study Commission in the U.S. supported the view that "the Social Security Number is a surrogate for the problem of record linkage, exchange and consolidation," it rejected the idea of repealing the section of the Privacy Act restricting the use of the Social Security Number because the section "may be somewhat successful

33 French Law No. 78-17, Concerning Data Processing, Files and Liberties (1978), Article 18, as translated in U.S. Department of Commerce, Office of Telecommunications, Selected Foreign National Data Protection Laws and Bills (Washington, D.C.: U.S.G.P.O., 1978) 43-44.

34 "The Personal Number Stymied in Germany?" Transnational Data Reports I, (2) (May, 1978) 18.

35 See supra note 32, 264.

36 Privacy Act, U.S. Public Law 93-579 (1974), s. 7.

in alleviating citizens' concerns about the 'dossier building' capacity in government."³⁷ At the state level, both Arkansas and Virginia restrict collection of the Social Security Number by government and quasi-government agencies, and prohibit such agencies from refusing services or privileges to any individual who does not furnish the number.³⁸ Florida prohibits use of the number as any customer's personal identifier by banks operating automated funds transfer systems.³⁹ Neither Canada nor Ontario have such legislative moratoria.⁴⁰

Other more unusual devices for protecting citizens from unauthorized use and dissemination of Social Insurance Numbers have been proposed by experts on the subject. An interesting temporary answer to the problem has been suggested by Professor Eric Manning of the University of Waterloo (in a presentation to the Commission on Freedom of Information and Individual Privacy, June 6, 1979). Disturbed by the spread of massive government and private data banks, and by the absence

37 U.S. Privacy Protection Study Commission, op.cit., 613. By the term "surrogate," the PPSC was referring to the tendency in the public mind to associate a complex set of issues about record linkage with the more specific problem of the use of single identifying numbers.

38 Arkansas Information Practices Act, 1976, s. 16-807; and Virginia Privacy Protection Act of 1976, c. 597, s. 2.1-385.

39 Florida Statutes Annotated, 659.062.

40 However, at the national level, the Conservative government planned to introduce legislation to: reduce the number of federal information banks that may legally use Social Insurance Numbers for identification; specify legitimate uses for the numbers; and ensure that those who refuse to give their numbers are not penalized in situations where demanding the number is illegal.

of technical and legal data protection mechanisms for individuals in Ontario, Professor Manning recommended that unique personal identification numbers be issued to every Canadian. These numbers would become the private property of the recipients.⁴¹

Whatever the ultimate solution to the problem of single identifying numbers, it is important that input from the public at large and from organizations and individuals concerned about privacy be solicited and seriously considered. The British Lindop Committee recommended that a universal personal identifier not be permitted to become a reality merely through ever-expanding use, by many organizations, of a convenient existing identifier such as a Social Insurance Number. If a universal personal identifier were ever seriously contemplated by the British government, the Committee saw the need to establish an independent committee to consider its privacy implications and the need to enact special legislation prior to the number's adoption.

Some European countries have submitted the question of standard personal registration numbers or systems to a parliamentary debate and vote (e.g., France, Germany, the Netherlands).⁴² The conclusion of the 1972

41 As private property, the number and its use would be completely controlled by the owner. Any person or agency wishing to collect, register or use the number would have to obtain the owner's prior written authorization, or risk both criminal and civil sanctions. If adequate technical and legal safeguards for personal data were implemented in Ontario, Professor Manning believes this temporary solution would no longer be necessary.

42 Hondius, Frits, op.cit., 23-53.

Report on Privacy and Computers emphasized the need for a public evaluation and decision regarding adoption of a single identifying number:

It is possible that a de facto personal identification number will develop in Canada, either through an ever-widening use of the Social Insurance Number (despite its limitations) or indirectly through credit card and bank account numbers. However, it is important to ensure that a single identifying number should not be adopted in Canada, directly or indirectly, without a full explanation and public debate of its merits and consequences.

43

Solutions to some of the problems surrounding records linkage, exchange and consolidation are proposed in Chapter VII of this report. However, as far as single identifying numbers are concerned, we would make the following specific suggestions to the Commission:

1) The indiscriminate use of the Social Insurance Number for many purposes is heading inexorably towards the de facto creation of a single identifying number in Canada. There is no evidence that any action is being taken at the federal level to prevent a personal registration system from becoming a reality. Indeed, such moves as the requirement of a Social Insurance Number for the cashing of Canada Savings Bonds will likely further extend the application of the number to members of the population such as youth and homemakers who have never needed it before. We did not attempt to assess the reasoning

43 Canada, Departments of Communications and Justice, Privacy and Computers (Ottawa: Queen's Printer, 1972) 89.

behind apparent federal government policies regarding the Social Insurance Number. From the point of view of the Ontario government, however, it would appear to us that the safest strategy, at least until improved policies regarding third party access to records and the physical security of personal records are in place, would be for each area not related to employment, pensions or taxation to develop its own Unique Personal Identifiers, rather than to rely on a single identifying number, such as the Social Insurance Number, the use and dissemination of which is not provincially controlled. At this point, we do not know what consequences will arise from Ontario's wholesale adoption of the Social Insurance Number. However, the threat of privacy-invasive consequences is sufficient that we recommend provincial agencies err on the side of caution.

2) An added protection to the individual against the collection of Social Insurance Numbers by agencies for whom the number was not originally intended by law, would be to grant to the individual a right of refusal to divulge the number to such agencies. In addition, agencies would be prohibited from denying any benefit or service for refusing to reveal the number. These rights would provide the individual with some measure of control over the use of numbers associated with him/her, except for uses previously authorized by statute.

3) To prevent further abuses of privacy, identifying numbers should be specifically described as to their purpose and approved uses, in legislation or in the regulations to statutes governing the programs for which the numbers are designated. However, legislation is unlikely to bring about reforms unless serious sanctions for unauthorized dissemination or misappropriation of the numbers are invoked.

There would, of course, be administrative implications to these suggestions, which we have not been able to assess. It may require rolling back the use of Social Insurance Numbers by some agencies and more clearly defining the purposes and uses of personal identifiers on the part of all agencies. One of the suggestions we make in Chapter VII concerning overall data protection is the creation of a Data Protection Board. Such an agency could provide helpful advice and guidance to government programs in implementing our suggestions for controlling the use of single identifying numbers, and could serve as a forum for public input and debate about the issue.

CHAPTER VI

LEGISLATIVE APPROACHES TO PRIVACY AND DATA PROTECTION

When we speak of legislation to resolve the informational privacy problem, we have by no means defined a solution. The legislature could select from quite a broad range of schemes to deal with some or all of the issues raised under the umbrella of "informational privacy." To illustrate the variety of choices which could be made, we examine here some of the schemes in place in other jurisdictions which have already addressed the issue through legislation. Although the alternatives are not exhausted in the examples chosen, the following discussion will familiarize the reader with the most commonly adopted mechanisms for the protection of privacy with respect to personal information-handling in what increasingly seems to be the "age of information."

Three basic approaches may be identified among the many legislative enactments, the stated purpose of which involves the protection of privacy. These may be referred to as the "tort" approach, the "public awareness/ombudsman" approach, and the "data regulation" approach.

A. The Tort Approach: Creating
Private Rights of Action

Some jurisdictions have attempted to redress privacy problems by recognizing "invasion of privacy" as an actionable wrong. This has the effect of permitting one whose privacy has been invaded to bring a lawsuit against the invader and recover damages. In Manitoba, Saskatchewan and British Columbia, the provincial legislatures have enacted statutes creating torts of privacy invasion. Manitoba's Privacy Act,¹ was passed in 1970, and defines the wrongful act thus:

A person who substantially, unreasonably and without claim of right, violates the privacy of another person commits a² tort against that person.

There need be no proof of damage, which signifies that the wrongful act is not merely the loss of material value through an act known as "violation of privacy," but that the act itself is sufficient to occasion an "injury" compensable in damages.

Similarly, in British Columbia, it was enacted in 1968³ that:

It is a tort, actionable without proof of damage, for a person wilfully and without a claim of right, to violate the privacy⁴ of another.

1 Privacy Act, S.M. 1970, c. 74.

2 Ibid., s. 2(1).

3 Privacy Act, S.B.C. 1968, c. 39.

4 Ibid., s. 2(1).

The "privacy" thus enshrined is defined in different fashion by each act. In each case, the term is broadly and loosely defined. In British Columbia, for example, the "nature and degree" of privacy is defined as what is "reasonable in the circumstances."⁵ Other sections suggest that the primary intent of the statute is to restrict physical invasions of privacy by way of eavesdropping, surveillance, and the unauthorized use of another's likeness for profit motive.⁶

The Manitoba Act gives four examples of what violation of privacy may be "without limiting the generality" of the foregoing definition. As in British Columbia, it is indicated that the offending acts include surveillance and eavesdropping activity, and the unauthorized use of another's likeness for "purposes of gain to the user."⁷ The fourth example -- the unauthorized use of letters, diaries and other personal documents⁸ -- is not covered by the British Columbia Act and approaches the concept of informational privacy which is the primary concern of this Commission. The concept of privacy violated in this way is perhaps more subtle than the physical invasions set forth in the first three. Yet, the Act still does not deal with the inappropriate or unauthorized handling of information which has been released to another (especially where the other is the government), and integrated into an information

5 Ibid., s. 2(2).

6 Ibid., ss. 2(3), 4(1).

7 Privacy Act, S.M. 1970, c. 74, s 3(a), (b), (c).

8 Ibid., s. 3(d).

system (especially where that system is automated). It is this type of privacy violation with which this Commission is most concerned.

It is interesting to compare this statutory approach to the tort of privacy invasion with the development of the notion of privacy at common law, as conceived by American lawyers Samuel Warren and Louis Brandeis in 1890, and a later American scholar, W.L. Prosser, during this century. Warren and Brandeis analyzed a body of traditional tort law and offered the thesis that an independent value of privacy protection could be discerned beneath the surface of the case law. In their view, privacy should be recognized as an independent value, not merely as an aspect of the values preserved by such traditional torts as trespass or defamation, and one whose redress lies in a tort remedy.⁹ Invasion of privacy was thus recognized by Warren and Brandeis as an independent actionable wrong. The underlying notion, presumably, was one capable of extension to new and evolving forms of privacy invasion. Prosser's later analysis, however, offered a rather different view of the common law cases. In place of the one tort of privacy invasion, Prosser argued that the case law could be broken down into a "complex of four" distinct torts.¹⁰ Whatever the merits of Prosser's analysis as a device for understanding the existing case law, it is arguable that his analysis has reduced the protection of

9 Warren, Samuel D. and Brandeis, Louis D., The Right to Privacy (1890), 4 Harvard Law Review 289.

10 Prosser, William L., Privacy (1960), 48 California Law Review 383.

privacy from the independent but neglected right envisaged by Warren and Brandeis to something which is merely an element of traditional legal rights. Prosser thus appears to offer an analysis which limits the capacity of the concept of privacy invasion to adopt to newer forms of privacy invasion.

The enumeration, in both the Manitoba and British Columbia Acts, of violations of privacy parallel closely the following categories of privacy put forth by Prosser:

- 1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;
- 2) Public disclosure of embarrassing facts about the plaintiff;
- 3) Publicity which places the plaintiff in a "false light" in the public eye;
- 4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness. 11

By reducing the general concept of "privacy invasion" into these four categories of more traditional tort law, Prosser avoids recognition of the uniqueness of privacy per se as an aspect of human life which is worthy of legal protection in a general fashion. Prosser's approach does not yield a principle of privacy protection from which we can extrapolate protection from the modern demon of information abuse through the storage and transfer of personal data in government files. In short, it seems incapable of offering an adequate theoretical basis for fully addressing privacy concerns in the information age.

11 Ibid., 389.

The one virtue of the Canadian provincial statutes is that they give protection in areas where the common law of tort has been reluctant to give redress.¹² Nonetheless, these statutory remedies have serious shortcomings. Jeremy Williams states them concisely:

One is that the plaintiff may never know that his privacy has been intruded upon. The other is that all these private law remedies are costly, slow and only serve to redress damage already done. 13

In fact, only one reported case decided under any of these statutes has come to our attention.¹⁴ There, although the plaintiff was awarded damages at trial as a result of private surveillance of him by means of a "bumper beeper," the decision was overturned on appeal. It was found by the courts that in the circumstances (divorce proceedings), such surveillance did not constitute an unreasonable invasion of privacy.

In sum, the enactment of a statute creating a tort remedy for violation of privacy does not appear to be an adequate response to the informational privacy problem. Its theoretical basis is questionable, making its application to informational privacy rather doubtful. More significant, though, is the difficulty in utilizing the remedy. Especially in the context of automated information manipulation, the onus on a plaintiff discovering a violation of his/her privacy and initiating a civil action would, as one commentator has said, "foredoom it to failure."¹⁵

12 Krouse v. Chrysler, (1970) 12 D.L.R. (3d) 463.

13 Williams, Jeremy, Invasion of Privacy (1973), 9 Alta. L. Rev. 11 at 10.

14 Davis v. McArthur, (1971) 17 D.L.R. (3d) 760.

15 Saxe, Diane, Data Protection and Government Information Handling (Toronto: Ministry of Energy, 1976) 41.

B. The Ombudsman Approach

Another approach to privacy protection is exemplified in New South Wales, Australia, where a Privacy Committee was established by legislation in 1975.¹⁶ A standing committee of the Australian Attorney General's Department had reported in 1973 on the subject of privacy.¹⁷ Its general conclusion was that the popular concern about privacy was more in response to an ill-defined perception of a problem, rather than to specific violations of privacy. The use of tort law was said to be inappropriate, since tort law can deal only with material violations of privacy on a case-by-case basis. The concerns perceived by the committee were not bounded by precise definition; they were thought to be more of an intangible nature, a reaction to "living in a complex society."

Following the committee's recommendations, the legislation adopted created a permanent Privacy Committee to investigate, mediate and recommend solutions in matters of alleged privacy invasions. A pamphlet explains:

A general privacy law could cause uncertainty until a large body of supplementary case law developed. The result could be a law offering spasmodic and uneven protection. Other problems are that the social context of many privacy problems are little understood, the proper boundaries of privacy are open to debate, and the field of privacy is subject to rapid social and technological change. The majority of privacy issues can be resolved by the Committee without recourse to legal proceedings.¹⁸

16 New South Wales, Australia, Privacy Committee Act, 1975. no. 37.

17 Morison, W.L., Report on the Law of Privacy, Parliament of New South Wales, Australia, 1973.

18 Introducing the Privacy Committee (Sydney, New South Wales, Australia: Privacy Committee, 1978). The Privacy Committee Act, s. 15, sets out the Committee's powers. It

(cont'd)

The composition of the Committee is prescribed by statute,¹⁹ and is comprised of 12 to 15 members, of whom one must be the Ombudsman,²⁰ and one the Executive Member. Of the remaining members, two are appointed by the Governor from elected members of the legislature, with one nominated by the Leader of the Opposition and one by the responsible minister;

18 (cont'd)

(a) may conduct research and collect and collate information in respect of any matter relating to the privacy of persons;

(b) may and, if directed by the Minister so to do, shall make reports and recommendations to the Minister in relation to any matter that concerns the need for or the desirability of legislative or administrative action in the interests of the privacy of persons;

(c) may make reports and recommendations to any person in relation to any matter that concerns the need for or the desirability of action by that person in the interests of the privacy of persons;

(d) may receive and investigate complaints about alleged violations of the privacy of persons and in respect thereof may make reports to complainants;

(e) may, in relation to any matter relating to the privacy of persons generally, disseminate information and undertake educational work;

(f) may, in relation to any matter relating to the privacy of persons generally, make public statements; and

(g) may, for the purposes of this Act, conduct such inquiries and make such investigations as it thinks fit.

19 New South Wales, Australia, Privacy Committee Act, 1975, no. 37, s. 5(4)(e).

20 The Ombudsman is appointed to a seven-year term, under The Ombudsman Act, 1974.

Their function is to receive and investigate complaints about alleged irregular or inequitable administrative decisions and actions of government organizations.

Review of New South Wales Government Administration, Directions for Change, Interim Report (Sydney, New South Wales: Government Printer, 1977) 279.

two are members of the public service, two are university faculty members, and the others are persons nominated by the Minister as having "special knowledge of or interest in matters affecting the privacy of persons."

The Committee thus constituted has power to delegate its powers to subcommittees. In fact, it is the subcommittees which perform most of the Committee's statutory functions. Primarily, the bulk of the Committee's energies are absorbed in its complaints investigation and research functions.

The Committee is vested with a power to require the production of documents and the appearance of witnesses, similar to the powers of a Royal Commission.²¹ Certain rules of evidence applicable to court proceedings are imported to the Act as exemptions to these powers. As a general rule, however, it is our understanding that this power to conduct investigations is infrequently, if ever, utilized by the Committee. The approach adopted by the Committee has been to place priority on seeking cooperation and on voluntary assumption of responsibility to avoid privacy intrusive practices. It appears to be the Committee's view that measures undertaken in an atmosphere of voluntarism are more likely to be effective (and economical) than measures undertaken in an atmosphere of coercion. Self-regulation undertaken in a cooperative spirit is thought to have the advantage of

21 New South Wales, Australia, Privacy Committee Act, 1975, no. 37, s. 16.

permitting individual solutions tailored to the needs and problems of the particular industry or institution. Further, it is felt that the regulatee is more likely to be committed to the solution in question if it has been fashioned and adopted in this manner.²²

Because of its broadly constituted powers relating to "the privacy of persons," the Committee researches and reports on matters pertaining to both the private and public sectors. Currently, it is working on three major research projects: Personal Data Systems, Criminal Records, and Privacy Aspects of Employment Practices. Already, guidelines concerning administrative and business practices have achieved change in the areas of credit, criminal, medical and employment records.

The Privacy Committee appears to have enjoyed considerable success in achieving complaint resolution and the voluntary adoption of codes of behaviour. The Committee's work thus represents an interesting and illuminating experiment in mediation and self-regulation as a solution to the privacy protection problem. In our view, the Committee's success may be attributed in large part to three factors. First, the fact that the failure of a scheme dependent on conciliation and self-regulation might ultimately lead to the enactment of comprehensive data protection laws might provide a tacit, but effective, incentive for a cooperative response from affected parties. Second, the interest of the mass media in following the research and recommendations of the Committee appears to have had an impact on the community at large. Many of the Committee's

22 Interview with Mr. W.J. Orme, Executive Member of the Privacy Committee, New South Wales (Toronto: July 5, 1978).

recommendations may thus have a bearing on the public image of the alleged privacy invader; relatively few, however, materially affect the efficient operation of an organization. The prospect of a public relations problem may therefore tip the balance in favour of implementing the Committee's recommendations. As the Committee puts it:

There is ... a growing awareness that it is in an organization's own interests to avoid unjustified invasions in order to maintain sales, improve employee relations and obtain the best data from surveys. 23

The third factor is a personal one. The charismatic personality and abundant enthusiasm of the present Executive Member of the Committee appears to be instrumental in effecting a solution in most cases. The Executive Member personally negotiates a solution to most problem cases. In fact, only 2-1/2% of the cases result in recommendations of the Committee.

While the New South Wales approach thus does offer some promise -- if only as an intermediate or interim solution -- it is our view that there are a number of difficulties with it. First, the fact that the bulk of recommendations made by the Committee stems from complaints means that in the absence of complaints, an area of privacy invasion may be overlooked. The research program appears to cover many broad problem areas, but where individuals suffering from invasive practices do not have the sophistication necessary to express the concern, important

issues may be neglected. A case in point is the treatment of welfare recipient records. Although this has been identified as a matter of particular concern by this study, the Privacy Committee appears thus far to have undertaken no work in this area. No research reports have been commissioned; nor does the Executive Member know of any complaints in this area. The extent of privacy invasion documented in our study in the social service delivery systems, generally leads one to suspect that the absence of complaints from New South Wales recipients is due to a lack of knowledge or motivation which would be necessary to effectively use the resources of the Privacy Committee.

Another difficulty with such a scheme is the somewhat piecemeal effect derived from the composite of solutions. Although it may be a purpose of the scheme to avoid consistency for its own sake and address each problem on its own terms, it is difficult to understand how the Committee's stated purpose of developing general definitions and criteria for privacy legislation can be achieved this way. A series of ad hoc solutions to complaints may give some global picture of what the range of "privacy problems" may be, but without guiding principles, it cannot be expected that a unified approach to privacy protection can be extrapolated. The Privacy Committee may conclude that a unified approach is unrealistic and undesirable. This result does, however, seem almost to be dictated by the process of accumulating ad hoc solutions to individual complaints.

C. The Data Regulation Approach

The legislation concerning privacy protection we have examined thus far takes a broad view of the nature of the privacy interests needing protection. The New South Wales scheme, for example, has as one of its purposes, the discovery of interests which can be labelled as private and in need of protection. The next group of statutes to be examined narrows its object to what Alan Westin has termed "informational privacy."²⁴ This focus corresponds more closely to the primary interest of this study -- the handling of personal information by government.

The common premise of the statutes examined in this section is that as increasing quantities and types of personal information are collected by the private and public sectors, and as computers are used more extensively, the potential for abuse and consequent unwarranted invasion of individual privacy increases.²⁵ The collection of personal data and its storage, retrieval and manipulation through automated means are trends which are likely only to increase. No privacy scheme has proposed to roll back this trend. But legislative measures have been proposed and adopted to curb the perceived dangers inherent in these developments.

24 Westin, Alan, Privacy and Freedom (New York: Atheneum, 1967) 7. Dr. Westin proposed the following as his definition of privacy:

Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

25 See Chapter IV of this paper, entitled "Computers and Government Records."

There are two major schools of thought determining two different starting points for the intervention of legislative dictates in the interests of privacy. The first fixates on storage and transfer of personal information as the critical areas of concern. A European privacy expert, F.W. Hondius, states that this "strict view" of data protection makes "keepers and operators of data banks ... responsible for the good quality and proper handling of the information which is under their effective control for as long as it is under their control." The second or "broader view," in Hondius' terms, envisages that:

... data protection should start from the moment when data are obtained, even before they are placed in storage. Verification of the accuracy of the data, which belongs to the duties imposed on data bank keepers by data protection law, will be facilitated by knowledge about the way in which data have been acquired. 26

Although this dichotomy of approaches does not match perfectly the range of privacy statutes examined in this chapter, there is, nonetheless, a distinction to be drawn between the two groups on the basis of the point at which controls intervene in the information flow. The North American statutes control only "proper handling," in accordance with Hondius' strict view. The European schemes, on the other hand, impose controls on data processing operations at an earlier stage — though they do not attempt to control methods of collection — than does the North American legislation. The degree of government control through legislation for the purposes of administration and enforcement is much higher in the European schemes.

26 Hondius, Frits, Emerging Data Protection in Europe (New York: American Elsevier Publishing Co., 1975) 107-110.

There are common features to nearly all statutes in the group now to be examined. These features create a convenient framework for the following discussion:

- . General description of statutes
- . Collection and storage of personal information
- . Transfer, subject access, and corrections
- . Enforcement and administration.

Under the first heading, a very brief overview will be given of the legislation in force in the jurisdictions to be considered -- Sweden, France, Germany, the United States and Canada. More detailed accounts of the approach taken in each jurisdiction to the three specific topic headings will follow.

1. General Description of Statutes

a) Sweden

The Swedish Data Bank Statute was enacted in May, 1973. Under the Act, the establishment or continuance of a "register of persons" by any public authority or private institution, such as a business corporation, is subject to monitoring by the Data Inspection Board (DIB),²⁷ a supervisory agency established by the statute. A register of persons

27 The Swedish Data Bank Statute, 1973, c. 289, s. 2. References in this paper to this statute are to the English translations in Selected Foreign National Data Protection Laws and Bills, Charles K. Wilk, ed., (Washington, D.C.: USGPO, Dept. of Commerce, Office of Telecommunications, 1978).

maintains personal information by means of automatic data processing. Permission must be sought from the Data Inspection Board to operate a register of persons. Details of the system must be submitted for a determination of whether "undue encroachment on privacy of the individuals registered" will result from the system's operation.²⁸ Although the law applies to both private and public sector data operations, it must be noted that registers established by executive or legislative direction are subject only to the opinion of the Data Inspection Board. They need not get the DIB's approval in the form of a licence. In practice, this effectively exempts government banks from direct DIB regulation.

Once a particular system has been approved by the Board, a "registrar-accountable" must be named within the organization maintaining the register.²⁹ That person is responsible for the lawful operation of the register, in accordance with the terms of the licence. The DIB's power with respect to the licence allows it to issue regulations in the following matters:

- 1) obtaining information for the register of persons;
 - 2) carrying out electronic data processing;
 - 3) technical equipment;
 - 4) processing of information on persons in the register in regard to automatic data processing;
 - 5) information (sent) to persons affected;
 - 6) information on persons which may be made available;
 - 7) distribution and other use of information on persons;
 - 8) storage and weeding out of information on persons; and
 - 9) control and security.
- 30

28 Swedish Data Bank Statute, 1973, c. 289, s. 3.

29 Ibid., ss. 8-14.

30 Ibid., ss. 5, 6.

b) France

France enacted its Law Concerning Data Processing, Files and Liberties in January, 1978. It created a National Commission on Data Processing and Liberties.³¹ This is an independant administrative authority with a mandate to exercise a regulatory power over the processes of nominative (personally identifiable) data,³² and to enforce the law through its licensing and public education powers.

In essence, three different statutory schemes are established by the Act. Government data operations must be specifically approved by an opinion issued by the National Commission.³³ Data processing for other than the government or the public service may be undertaken upon declaration of conformity with the applicable law.³⁴ The third category of regulation requires a simplified declaration for the most routine operations of a public or private nature that obviously do not affect private life or liberties.³⁵ For all nominative data processing operations, applications must be submitted to the Commission for approval. For such operations on behalf of the government, terms are set out in a licence. The statute calls for a publication describing

31 French Data Act, article 6.

32 Ibid., article 5.

33 Ibid., article 15.

34 Ibid., article 16.

35 Ibid., article 17.

approved operations.³⁶ A procedure for subject access and data correction is set out.³⁷ The various duties of the Commission will be described in a later section of this chapter.³⁸

c) Federal Republic of Germany

The data protection scheme imposed in the German Federal Republic in 1977³⁹ is less comprehensive in its approach than the statutes we examined in Sweden and France. The general premise of the Law for the Protection of Personal Data Against Misuse in Data Processing is that processing of personal data is permissible where "expressly authorized by statute," or with the written consent of the data subject.⁴⁰ Automatic data processing and some manually-kept files are covered by the law.⁴¹

The German statute sets out obligations for data processors, which

36 Ibid., article 22.

37 Ibid., articles 34-40. See infra, pp. 133-135.

38 Ibid., articles 14-17, 21-24. See infra, pp. 160-162.

39 German Federal Republic, Federal Data Protection Act of January 27, 1977. References in this paper to this statute are to the English translation in Selected Foreign National Data Protection Laws and Bills, op. cit., note 27.

40 Federal Data Protection Act, s. 3.

41 Ibid., ss. 2(2)(1) and 2(3)(3).

vary according to the identity of the data processor and purpose of the operation. Three groups of processors identified are:

- 1) authorities and other public agencies of the Federation, corporations directly under the Federation, institutes and foundations of the public law, as well as associations of such corporations, institutes and foundations; 42
- 2) natural persons and legal entities, corporations and other personal associations of private law, whose data processing operations are for their own business purposes; 43
- 3) the groups named in the second paragraph, where the data processing operation is for the benefit of third parties. 44

The statute is designed to yield to provincial (Länder) legislation.⁴⁵
The requirements of the Act are administered by a Federal Commissioner in relation to the first group of registers, and by provincial supervisory authorities for the others.⁴⁶ Authorities and public

42 Ibid., s. 7(1) (Chapter 2).

43 Ibid., s. 22 (Chapter 3).

44 Ibid., s. 31 (Chapter 4).

45 Ibid., s. 7(2). This part of the act is designed to give way to similar laws passed by the "Länder" (provinces):

Insofar as data protection is not governed by land law, the provisions of the present chapter ... also shall apply to:

(1) authorities and other public agencies of the Länder, municipalities and their associations, and other legal entities of public law under the supervision of the Land, and to associations if these implement federal law;

(2) authorities and other public agencies of the Länder insofar as they function as organs of the administration of justice.

46 Ibid. See infra, pp. 162-165.

agencies must publish in the Official Gazette specified details about stored personal data.⁴⁷ Police, military and revenue authorities are exempt from this requirement.⁴⁸ The second group of "non-public agencies" must assure that a data subject knows of data stored about him/her.⁴⁹ Procedures for access and correction are set out in relation to each category of data operation.⁵⁰

d) United States of America

The stated purpose of the Privacy Act of 1974⁵¹ is to provide safeguards for an individual against an invasion of personal privacy by a federal agency which holds information about the individual.⁵² Federal agencies must permit an individual to know what records are maintained about him/her; they must allow such records to be used only

47 Ibid., s. 12(1).

48 Ibid., s. 12(2).

49 Ibid., s. 26(1).

50 See infra, pp. 136-141.

51 Privacy Act, 1974, 5 U.S.C., s. 552a, passed as part of Pub. L. No. 93-579.

52 Privacy Act, 1974, Pub. L. No. 93-579, s. 2(b) states that:

The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring federal agencies, except as otherwise provided by law, to:

(1) permit an individual to determine what records pertaining to him are collected, maintained, used or disseminated by such agencies;

(cont'd)

for purposes to which s/he has consented; and must permit an individual access to, copies of, and a means of correcting records.⁵³ The structure of this Act obviously places emphasis on individual initiative as the principal means of assuring the protection of privacy.

The Act followed a study by the Department of Health, Education and Welfare in 1972, which proposed guidelines for information handling by government agencies. These guidelines were "refined" to eight principles by the Privacy Protection Study Commission (PPSC). This Commission was set up by the Privacy Act to examine the implementation of the Privacy Act by agencies, and to study problems of record

52 (cont'd)

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemptions as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of wilful or intentional action which violates any individual's rights under this Act.

53 Ibid., s. 552a(è).

privacy in the private sector. The principles which they see as underlying the provisions of the Act are as follows:

(1) There shall be no personal-data record-keeping system whose very existence is secret and there shall be a policy of openness about an organization's personal-data record-keeping policies, practices, and systems.

(The Openness Principle)

(2) An individual about whom information is maintained by a record-keeping organization in individually identifiable form shall have a right to see and copy that information.

(The Individual Access Principle)

(3) An individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information.

(The Individual Participation Principle)

(4) There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information.

(The Collection Limitation Principle)

(5) There shall be limits on the internal uses of information about an individual within a record-keeping organization.

(The Use Limitation Principle)

(6) There shall be limits on the external disclosures of information about an individual a record-keeping organization may make.

(The Disclosure Limitation Principle)

(7) A record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate.

(The Information Management Principle)

(8) A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems.

(The Accountability Principle)

54

54 Privacy Protection Study Commission, Appendix 4, The Privacy Act of 1974: An Assessment (Washington, D.C.: USGPO, 1977) 76, (hereafter, Appendix 4). The Study Commission was authorized by Public Law No. 93-579.

e) Canada

The initiative of the federal Canadian government into the field of personal data control is in the guise of the Canadian Human Rights Act, Part IV.⁵⁵ This legislation came into force in March, 1978. The purpose of Part IV is to guarantee "to individuals rights of access and correction with respect to personal information held about them by the federal government,"⁵⁶ its departments and agencies, and to control the use to which this information is put, and its accuracy. (Other Parts of the Act deal with prohibited grounds of discrimination, and are not of relevance here).

Part IV requires the publication of an Index describing all "Federal Information Banks,"⁵⁷ which are stores of personal information maintained by the Canadian government for use in decision-making processes. A procedure is set out for subject access to and correction of this data.⁵⁸ A supervisory authority is given to the Treasury Board, the federal government agency primarily responsible for financial administration, to oversee future collection and storage of personal information.

55 Canadian Human Rights Act, S.C. 1976-77, c. 33.

56 Press Release, materials distributed in March, 1978.

57 Ibid., c. 33, s. 51.

58 Ibid., c. 33, s. 52. See infra, pp. 150-153.

2. Collection and Storage of Personal Information

The first step in the information process is the collection of data. Although not all statutes examined here deal with this step of the process, the obvious importance to the individual of what is gathered and fed into a data processing operation has been recognized widely. The Council of Europe has stated in its Resolution concerning public sector data banks that:

2. The information stored should be:

- (a) obtained by lawful and fair means;
- (b) accurate and kept up-to-date;
- (c) appropriate and relevant to the purpose for which it has been stored.

Every care should be taken to correct inaccurate information and to erase inappropriate, irrelevant or obsolete information.

3. Especially when electronic data banks process information relating to the intimate private life of individuals or when the processing of information might lead to unfair discrimination,

- (a) their existence must have been provided for by law, or by special regulation or have been made public in a statement or document, in accordance with the legal system of each member state;
- (b) such law, regulation, statement or document must clearly state the purpose of storage and use of such information, as well as the conditions under which it may be communicated either within the public administration or to private persons or bodies;
- (c) the data stored must not be used for purposes other than those which have been defined unless exception is explicitly permitted by law, is granted by a competent authority or the rules for the use of the electronic data bank are amended.

59

59 Council of Europe Resolution (74)29: "On the protection of privacy of individuals vis-a-vis electronic data banks in the public sector."

Concerning private sector data banks, the Council resolved that:

1. The information stored should be accurate and should be kept up-to-date.

In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.

2. The information should be appropriate and relevant with regard to the purpose for which it has been stored.

3. The information should not be obtained by fraudulent or unfair means. 60

Another aspect of record-keeping which is widely considered to affect the privacy abuse potential is the timeliness of data. This is reflected in the Council of Europe's resolution concerning public sector data operations, which states that

Rules should be laid down to specify the time-limits beyond which certain categories of information may not be kept or used. 61

This principle has as its objective the protection of the individual from the negative impact of information far beyond the time of its relevance. Human memory tends to erase certain information, especially when more recent information overcomes the original negative impact. Computer memories do not have this capacity to forgive through time. Hence, timeliness is an element of relevance which must be controlled independent of superficial relevance.

60 Council of Europe Resolution (73)22: "On the protection of privacy of individuals vis-a-vis electronic data banks in the private sector."

61 Council of Europe Resolution (74)29, para. 2.

a) Collection and Storage
in Sweden

Certain types of information may not be stored in a register of persons by "other than an authority responsible by law or statute for keeping a record of such information, unless there are extraordinary reasons therefor."⁶² These are the most sensitive types of data, which are most easily abused. They include information about criminal or psychiatric records, reliance on social welfare assistance, and health records (which may mention alcohol or drug dependence). Registers containing information on political or religious views will only be permitted where there are special reasons for it.

The application for a licence includes a description of the origin of the information destined for the register, and the means by which it will be collected.⁶³ Regulations in the licence must deal with the type of information to be entered in the register, and the means for its collection.⁶⁴

The Swedish Data Bank Statute makes no specific reference to timeliness of data, but the Regulation requires an applicant for the establishment of a register of persons to state how long records shall

62 Swedish Data Bank Statute, s. 4.

63 Ibid., Regulation of May 11, 1973, s. 2(4).

64 Ibid., s. 6.

be preserved, and how and when the "weeding" shall be undertaken.⁶⁵
Timeliness becomes a condition of the licence granted by the Data
Inspection Board, which is administered by the registrar-accountable.

b) Collection and Storage
in France

In similar fashion to the Swedes, the French arrest certain dangers
attendant on collecting and processing sensitive personal information
before they arise. Article 31 of the French law forbids the entry or
storage in a computer memory of data indicating "the racial origins
or political, philosophical or religious opinions or the trade union
membership of persons." The exception to the rule is where there is
consent to such storage by the data subject, or where the storing party
is a religious, political or trade union organization.

There is a statutory proscription on the gathering of data by "any
fraudulent, unfair or illicit means" which applies to non-automated
data collections in addition to automated ones.⁶⁶

Data subjects must be informed of the mandatory or optional nature of
answers to be registered subject to the law, the consequences for not

65 Ibid., Regulation, s. 2(10).

66 French Data Act, article 5.

answering, the recipients of the data, and the existence of the rights of access and correction.⁶⁷

In France, the duration of storage for information must be stated on the application for a National Commission opinion, or in the declaration to the Commission.⁶⁸ Once a data operation is approved on the basis of such information, nominative data may not be stored longer than the Commission's authorization permits.

c) Collection and Storage
in the Federal Republic of Germany

There is no screening or approval required for German data processing operations, as there is in Sweden and France. Collection of personal data is permitted with either statutory authorization or written consent from the data subject.⁶⁹ The only other statutory provision affecting collection of personal information is the notice published in the Official Gazette by the first group of authorities, indicating, among other things, the types of personal data stored, and their purposes.⁷⁰

67 Ibid., article 27.

68 Ibid., article 19.

69 Federal Data Protection Act, s. 3.

70 Ibid., s. 12.

Storage of personal information is regulated by measures relating to technical and physical security. These measures must be implemented at a rate reflecting the costliness of the measures in relation to the cost of the operation.⁷¹

In Germany, one of the rights of a data subject set out in section 4 of the statute allows the concerned party to block or delete data, when the conditions for their storage no longer exist.⁷² However, criteria for determination of an over-long storage period are not set out in the statute.

d) Collection and Storage
in the United States of America

Agencies are required to observe certain requirements at the collection stage of the information process. Agencies are directed by the Privacy Act to maintain their records (and collected information) in accord with the Act's version of the five principles enunciated by the 1972 HEW study.⁷³

Analagous to European restrictions on collection of certain sensitive information is the Privacy Act's proscription of unauthorized files

71 Ibid., s. 6.

72 Ibid., s. 4(3)(4).

73 Appendix 4, 76.

concerning the manner in which an individual exercises First Amendment rights.⁷⁴ The Act sets stipulations on the collection and use of Social Security Numbers.⁷⁵ According to the PPSC, neither limitation has noticeably affected collection practices, since there are gaping loopholes in the legislative language.⁷⁶

Other provisions affecting collection and maintenance of personal information require "affirmative steps" in the information management practices of agencies.⁷⁷ Agencies must use the data subject ("subject individual") as the source of information to the greatest extent practicable, where the information is used in a decision-making process concerning the individual.⁷⁸ Records shall be maintained with "only such information as is relevant and necessary" to lawful agency purposes.⁷⁹ Accuracy, relevance, timeliness and completeness are required in records to assure fairness.⁸⁰

These measures reflect what is described by the Privacy Protection Study Commission as a "collection limitation principle." The PPSC found

74 5 U.S.C. s. 552a(e) (7) .

75 Pub. L. No. 93-579, s. 7.

76 Appendix 4, 88.

77 Ibid., 95.

78 5 U.S.C. s. 552a(e) (7) .

79 5 U.S.C. s. 552a(e) (1) .

80 5 U.S.C. s 552a(e) (5) .

that there had been "a modest amount of revision and reduction of data collection forms and consequently a modest reduction in data collection itself;" otherwise, impact of the collection requirements had been minimal.⁸¹

Collection and maintenance of personal information by agencies may also be affected by the publication requirement. The Privacy Act requires agencies to compile and publish annually their rules about the contents and operations of systems of records. This report is published in the Federal Register.⁸² It is intended to assist public use and knowledge of agency records, and generally makes agencies more accountable for their record-keeping practices. This exercise forces internal house-cleaning of old or offensive stored data.

The PPSC described this requirement as partially fulfilling the "openness principle" of the Act. Although it conceded that the notices in the Federal Register are useful for allowing public scrutiny of record-keeping practices, and for internal management, the PPSC suggested that more detail is required if the notices are to "reflect more accurately the content or manner in which an agency maintains records."⁸³

81 Appendix 4, 81.

82 5 U.S.C. s 552a(e) (4).

83 Appendix 4, 81.

The American Privacy Act attempts to ensure the timeliness of records in two ways. First, the retention period of each system of records is part of the information which must be published in the Federal Register.⁸⁴ The second requirement is that agencies generally

maintain all records which are used by the agency in making any determination about any individual with ... timeliness ... as is reasonably necessary to assure fairness to the individual in the determination. 85

e) Collection and Storage
in Canada

There is little in Part IV of the Canadian Human Rights Act which regulates collection of personal information. There are only two references to the collection stage of the information process. One is in the section granting citizens the right to examine their own records. It says [Every individual is entitled to]

(c) examine each such record or a copy thereof whether or not that individual provided all or any of the information contained in the record. (emphasis added) 86

The reference to "collection" obliquely suggests the absence of any regulation of collection practices. The emphasis found in the American

84 5 U.S.C. s. 552a(e) (4) (E). This paragraph refers to "the policies and practices of the agency regarding storage, retrievability, access controls, retention and disposal of records."

85 5 U.S.C. s. 552a(e) (5).

86 Canadian Human Rights Act, S.C. 1976-77, s. 52(1) (c).

Privacy Act on the importance of the data subject as the source of information in decision-making⁸⁷ is absent from the Canadian statute.

The other reference to collection is in the context of the oversight function of the Treasury Board. A long-range goal of the Act is to create more efficient information practices. To this end, the Minister responsible for Treasury Board is to keep under review the collection practices of government institutions and eliminate unnecessary collection where possible.⁸⁸ What constitutes unnecessary collection is not stated, but the context, notwithstanding the title of the Act, suggests an orientation toward management coordination and efficiency rather than the protection of privacy.

A third feature of the Act may have some impact on the collection of personal data. This is the requirement upon the Treasury Board to publish an Index to government holdings of personal information which are subject to the Act, the "Index to Federal Information Banks."⁸⁹ Publicity may encourage the abandonment of unnecessary record-keeping. Of course, the primary objects of this publication requirement are to enable the individual to know what information is held about him/her, and to facilitate access to and correction of that information by the

87 5 U.S.C. s. 552a(e) (5).

88 Canadian Human Rights Act, s. 56(2) (3) names the "designated minister" to take responsibility for coordination of information banks. The Treasury Board was appointed as the designated minister by Statutory Instrument 78-33, dated March 22, 1978.

89 Canadian Human Rights Act, s. 51(1).

individual. By publishing the Index, the principle of holding no secret data banks about individuals is fulfilled.

The only reference to timeliness in Part IV of the Canadian Human Rights Act is in section 56(3), which requires ministerial approval for the formation of new information banks or substantial modification of existing ones "for the purpose [inter alia] of ... eliminating, wherever possible, any unnecessary collection of information." It is not clear, however, whether the objective of this provision is merely cost efficiency, or whether the intention is to avoid the abuse of personal information which may be caused in specific instances by the use of stale information. As in other areas, the Canadian legislation is vague on this point. Recent Treasury Board statements do indicate, however, an awareness of the need to concentrate attention on the time of storage and use of data.⁹⁰

3. Transfer, Subject Access and Correction

The next cluster of issues for our examination in data privacy statutes centres on transfers of personal data by a record-keeping agency. These transfers may be within the collecting agency, to other arms of the collecting government or corporation, to unrelated outsiders, or to the data subject.

90 "Information Banks: Design and Collection," Administrative Policy Manual, chapter 410 (Ottawa: Treasury Board Canada, December, 1978).

The latter case is referred to here as subject access. In other instances, we talk about transfer of the record, although from another point of view, it is again a question of access. Limitations on transfers to the data subject or others may be a part of a data protection or privacy statute.

Mechanisms to assure the accuracy of data are discussed in this context. As we have seen, some statutes impose a duty upon the data collector to maintain accurate, timely, relevant, and/or complete files. To enforce this obligation, the data subject may be given a channel for checking the accuracy of files held about him/her. This would entail a procedure for making corrections. Additionally, an obligation may be imposed on data-keepers to transmit corrections to previous recipients, and in turn, an obligation may be imposed on those recipients to correct their files accordingly. Finally, record-keepers may be required to keep an accounting of transfers of information from the file. This accounting may or may not be available to the data subject.

The concept of allowing a person to know what personal information is held about him/her, to obtain a copy, and to ensure accuracy through an opportunity to make corrections has been widely advocated. The Council of Europe sets out this principle in its Resolution (74)29 "on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector." The principles to which member countries pledge to give effect, include these statements:

2 ... Every care should be taken to correct inaccurate information and to erase inappropriate, irrelevant or obsolete information.

3(c) ... data stored must not be used for purposes other than those which have been defined unless exception is explicitly permitted by law ...

5 ... Every individual should have the right to know the information stored about him.

8 ... When information is used for statistical purposes it should be released only in such a way that it is impossible to link information to a particular person. 91

In the United States, the Advisory Committee on Automated Personal Data Systems to the Secretary of Health, Education and Welfare recommended in 1972 a Code of Fair Information Practices. Four out of five principles deal with transfer and access:

There must be a way for an individual to find out what information about him is in a record and how it is used.

There must be a way for an individual to correct or amend a record of identifiable information about him.

There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data. 92

Several of the principles which the PPSC saw as underlying the Act deal with these same issues, namely:

91 Council of Europe Resolution (74)29.

92 Appendix 4.

The Individual Access Principle
The Individual Participation Principle
The Disclosure Limitation Principle 93
The Accountability Principle.

Similar principles are expressed in the Canadian statute. Generally,
the Act confers on Canadians a

right of access to records containing personal information
concerning them for any purpose including the purpose of 94
ensuring accuracy and completeness.

Specifically, section 52 states that every individual is entitled to:

- (b) ascertain the uses to which such records have been put
since the coming into force of this Part;
- (c) examine each such record or a copy thereof whether or not
that individual provided all or any of the information contained
in the record;
- (d) request correction of the contents of any such record where
that individual believes there is an error or omission therein;
and
- (e) require a notation on any such record of a requested
correction therein where the contents of such record are not
amended to reflect the requested correction.

Different means are used by different jurisdictions to implement the
principles underlying the individual's rights to access. What follows
is an outline of the mechanisms employed in Sweden, France, Germany,
the United States and Canada.

93 Appendix 4, 76.

94 Canadian Human Rights Act, S.C. 1976-77, c. 33, s. 2(b).

a) Transfer, Subject Access and
Correction in Sweden

The general rules on subject access and correction are stated in the Data Bank Statute itself, whereas provisions on transfer of personal data to third parties may be set forth in the terms of a particular licence. The administrative responsibility for implementing these rules falls on the registrar-accountable who is defined by the Act as the person who has control of the register and on whose behalf the register is maintained.⁹⁵ The registrar-accountable may be either a natural person or an organization.

Section 10 of the Act entitles the individual to know what information exists about him/her on the record. Presumably a person possesses this right in relation to each register containing information about him/her. Requests for information are made to the registrar-accountable who must reply "as soon as possible."⁹⁶ The registrar-accountable need only comply with such a request once in 12 months.⁹⁷

Exemptions to the general principle of subject access are provided for by subsection 10(3), which states that there is no obligation to

95 The Swedish Data Bank Statute defines the registrar-accountable as "anyone on whose behalf the register is maintained, provided that he also has control over the register." The duties of the registrar-accountable are set out in s. 8-14 of the Act.

96 Ibid., s. 10.

97 Ibid.

release information if there is a "law or statute or the decision of an authority" forbidding release to an individual. Just as some types of information may not be collected or stored in the first place, exempt material is pre-determined, and not subject to the expensive lengthy and contentious determinations which must be made in Canada or the United States upon the individual's request to access the material. A person who has obtained access to a file may become aware of incorrect information, and may wish to invoke the statutory duty imposed on the registrar-accountable to correct it. No procedures are set by statute for the correction of data or for resolution of disputes about the accuracy of data. However, in setting regulations for what data may be contained in a register, procedures for access and correction may also be devised.

Section 8 of the Act states that if there is "reason to suspect that information on persons is incorrect, the registrar-accountable shall without delay take the necessary steps to ascertain the correctness of the information" Corrections made in this way are to be transferred to previous recipients of the information.

A further duty assigned to the registrar-accountable is to take measures to ensure the completeness of information contained in the register. The duty is expressed to require that "the registrar-accountable should undertake what is necessary to complete a register of persons" (emphasis added).⁹⁸ However, if the lack of

98 Ibid., s. 9.

completeness may result in an undue encroachment of privacy or a risk of loss of rights, the duty is expressed in terms of a positive and binding obligation to act.

Although the question of third party access to personal files is dealt with by the DIB on a register-by-register basis through the terms and conditions of specific licences, there are a few provisions of the Act which impose limitations on such access. Section 11 forbids release of information "if there is reason to believe that the information will be used for electronic data processing without permission in accordance with this statute." Transfers abroad depend on permission from the Data Inspection Board, which will not be granted if the transfer may result in "undue encroachment" of privacy. As indicated above, if information has been released to a third party, the data subject may request that any deletions or changes made to the data since its release be reported to the third party recipient.⁹⁹ Further, the specific regulations governing a particular register may state that a third party recipient of information from the licensed register may not pass it on without authorization.¹⁰⁰

99 Ibid., s. 8.

100 Ibid., s. 13.

b) Transfer, Subject Access and
Correction in France

In France, the Law Concerning Data Processing, Files and Liberties includes under the heading of "Exercising the Right of Access" disclosure and correction provisions. These rights apply only to automated data processing.

An index required by article 22 may be used by a person wishing to know of the nominative data holdings governed by the Act. From the index, a person may determine which files contain information about him/her. The index sets out information about all automated data processing operations approved by the National Commission on Data Processing and Liberties. The publication indicates to whom inquiries shall be addressed in order to obtain access to the files, and indicates generally what type of data are contained in the data bank.

Only natural persons may exercise the right of access.¹⁰¹ The original bill had extended entitlement to all legal persons, but the corporate sector lobbied against this protection, apparently out of a desire to keep government regulation at a distance.¹⁰² Upon proof of identity, a person may exercise the right of access, and ascertain whether nominative data concerning him/her is processed in an operation

101 The French Data Act, article 4.

102 Interview with M. Louis Joinet, Member, Commission on Liberties, Files and Data Processing (Paris, December 19, 1978).

listed in the index. Disclosure of the data to the data subject may be obtained "if necessary,"¹⁰³ and article 35 sets forth the nature of the disclosure required. It must be in clear language and must conform to the contents of entries. A copy may be obtained upon payment of a sum set by the Commission. The Commission may allow a data-keeper to delay a response to an access request, or to refuse a request (inter alia, if many such requests are made). At the same time, if a person fears that data to which s/he has a right of access may be tampered with or deleted, an injunctive remedy against the data-keeper may be sought from the court.

Where access is desired regarding medical data, the interested party must designate a physician to receive the information for him/her.

The Act gives the data subject two means of assuring the accuracy of data, the processing and registration of which are subject to the Act. Article 36 allows the data subject to require "correction, completion, clarification, update or obliteration" of data. In addition to securing a high quality of data in the system, this article provides the means of removing proscribed information. The data subject thus has a personal role in policing the code set by article 31. If a person succeeds in modifying information, any fees paid for access must be reimbursed, and the data subject is entitled to a free copy of the new entry.

103 French Data Act, article 34.

Where a person requires correction to a file about him/her, and the file involves state security, defence or public safety, s/he petitions the Commission. It will investigate the matter and make necessary changes.¹⁰⁴

The second statutory assurance of correct data is contained in article 37, which places an obligation upon the data operation to maintain accurate, correct and complete data, regardless of how the inaccuracy is brought to its attention.¹⁰⁵

Upon modification or deletion of data, notification must be given to any third party who has previously received the data.¹⁰⁶ In contrast to the Swedish law, notification to third parties does not depend on the data subject's request. It must be done unless the Commission waives the requirement.

Transfer of data to third parties is also regulated. Certain third parties are authorized recipients of data, by virtue of the declaration made for initial authorization of the operation.¹⁰⁷ The identity of these authorized third parties is revealed to the data subject when information is solicited from him/her, and also by the Commission's

104 Ibid., article 39.

105 Ibid., article 29.

106 Ibid., article 38.

107 Ibid., article 20.

publication of processing operations.¹⁰⁸ These transfers are initially authorized by the Commission when it grants a licence, and the provisions are comparable to those for routine uses in the American statute, or derivative uses in the Canadian one.

Further, there is a general obligation placed upon persons responsible for nominative data processing under article 29, to "take all necessary precautions in order to preserve the security of the data, and especially to prevent their being distorted, damaged, or communicated to unauthorized third parties." In short, the French law attempts to ensure that a data subject is aware of the identity of parties who may receive nominative data about him/her, and that only correct and timely data is stored by all who receive it.

c) Transfer, Subject Access and
Correction in the Federal Republic of Germany

The German data processing law applies different access and correction rights to non-automated and automated data stored by the three categories of data-keepers -- public authorities, private parties processing data for internal use, and commercial parties processing data on behalf of others. Section 4 sets out four general rights granted under the Act. A person has a right to:

108 Ibid., articles 22, 27.

- 1) information about the stored data concerning his person;
- 2) correction of the stored data concerning his person if they are incorrect;
- 3) blocking of the stored data on his person if neither the correctness nor the incorrectness of the same can be established, or (he shall have such rights) after the conditions for their storage that originally had been met no longer exist;
- 4) deletion of the stored data concerning his person if their storage was not permissible or -- optionally besides the right to block -- after the originally met conditions for storage no longer exist.

The most elaborate provisions to enshrine section 4's statement of a right of subject access pertain to "the authorities and other public agencies." These are government departments, agencies and organizations akin to Crown corporations but which do not engage in competition.

A limited right of access is granted to a person about whom data is stored. The statutory requirement is only that "information ... on the stored data" be released.¹⁰⁹ The procedure and extent of disclosure are within the discretion of the storing agency. Exercise of the right of access may be facilitated to some extent by the requirement that notice of basic information concerning stored data be published¹¹⁰ in an official gazette. However, the publication requirement does not result in the preparation of a complete accounting of information with respect to all data banks, nor is all of the published information made available from one authoritative service.

109 Federal Data Protection Act, s. 13(1).

110 Ibid., s. 12(1).

A large group of "the authorities" is not bound by the notice sections. Military, police, judicial and taxation authorities need not publish notice of the personal data they hold.¹¹¹ A further group is exempted from the requirement of gazette publication. Registers authorized or created by statute or regulation are also exempt from notice requirements applying to public authorities if the basic information about their operation is specified either in published administrative guidelines, or as part of the statutory enactment creating them.¹¹²

There are exemptions from the general principle of subject access by agency and by protected interests. The access rules do not apply to military, police, judicial and taxation authorities. Further, material held by agencies subject to the access rules may be withheld:

- 1) where the information would "jeopardize the discharge of the duties" within the competence of the storing agency;
- 2) where public security or welfare may suffer;
- 3) where there are statutory secrecy requirements, or where the "overwhelming lawful interests of a third party" would be affected; or
- 4) where one of the exempt agencies is involved.

113

A further limitation on the access principle may result from the statute's requirement that an applicant specify in detail the data to which access is desired.

111 Ibid., ss. 12(2) (1), 13(2), 13(3) (2), 13(3) (3).

112 Ibid., s. 12(2) (3).

113 Ibid., s. 13(3).

The policy followed by public authorities in allowing access under the Act is to impose no fee. However, when access is available, fees may be imposed to cover direct administrative costs. The fee may be waived where the person wishing access successfully obtains correction or deletion of data.¹¹⁴

The statutory provision concerning correction rights is cast in broad terms. Section 14 states generally that "personal data shall be corrected if they are incorrect." No procedures for correction are set out in the statute. In disputed cases, the subject may invoke a statutory right to have the data "blocked." Where the correctness of data is disputed and incapable of resolution, or where the data are no longer required "for the lawful discharge of duties within [the authority's] competence," they are blocked -- no longer processed, transmitted, or otherwise used.¹¹⁵ Again, the Act does not stipulate procedures for making these determinations.

Modified requirements of notice, subject access and correction rights are applicable to the second category of data-keepers -- government controlled businesses, and private parties processing data for internal use.¹¹⁶ Although there is no publication requirement, notice to the party concerned with the data storage must be given upon first storage.¹¹⁷

114 Ibid., s. 13(4).

115 Ibid., s. 14(2).

116 Ibid., s. 22.

117 Ibid., s. 26.

Thereafter, a person may request information about data stored and other parties receiving the information. The exemptions from access here approximate those in the first category.¹¹⁸ The correction and blocking provision is identical to that for public authorities.¹¹⁹

Similar provisions apply to the third category -- commercial parties processing data on behalf of others.^{120, 121}

All categories of data operation in Germany are subject to transfer or "transmittal" restrictions. The limitations imposed on the first category, government agencies, are the least restrictive. Personal data may be transferred to "other government agencies or ecclesiastical associations under public law having facilities to ensure data security," where the data is necessary to the agency's functioning. Others may receive data if they establish a "legitimate interest" in the data.¹²²

118 Ibid., s. 26(4).

119 Ibid., s. 27.

120 Ibid., s. 31; s. 32(2) allows transfer of stored data to a recipient asserting a lawful interest in the data. The details of the interest must be placed on a record maintained by the transferor. Provision for notice to the data subject upon "first transmittal" is made in s. 34(1). The following subsections treat subject access to this type of data identically to the treatment of access to the second group (s. 26). Correction and blocking of data held by the third group of processors is handled in the same way as the second group also (s. 27).

121 Ibid., s. 34.

122 Ibid., ss. 10, 11.

Transfer of personal information stored by the second category of data processors are permissible within the bounds of any understanding with the data subject. In circumstances where the data is governed by some rule of confidentiality, the contract cannot derogate from that confidential status. For these data processors, strict requirements exist in order to transfer data containing "occupational and official secrets."¹²³

Commercial data processors may transfer data "where the recipient has demonstrated a legitimate interest in the knowledge thereof"¹²⁴ and where no harm would flow to the data subject.

Finally, rules of general application relating to the security of data are set out in an annex to the statute. Section 6 of the Act states, however, that "measures shall be required only if the expenditures are in a proportionate relationship with the protective goals to be achieved."¹²⁵

123 Ibid., s. 24.

124 Ibid., s. 32(2).

125 Annex to s. 6(1)1:

Should personal data be automatically processed, such measures shall be taken for the implementation of the provisions of the present law as are appropriate for the type of personal data to be protected:

- 1) to prevent access by unauthorized persons to data processing installations with which personal data are processed (access control);

(cont'd)

d) Transfer, Subject Access and
Correction in the United States of America

The American Privacy Act, as part of the administrative procedures legislation of the U.S. federal government, imposes privacy protection rules on the record-keeping practices of government agencies. Unlike the Swedish and French legislation, the Act does not affect control over the creation of data banks. Although, as the preceding discussion

125 (cont'd)

- 2) to prevent persons who are working on the processing of personal data from unauthorized removal of storage media (removal control);
- 3) to prevent unauthorized input into storage as well as the unauthorized taking, cognizance, altering, or deleting of stored personal data (storage control);
- 4) to prevent unauthorized persons from the use of data processing systems from or into which the personal data through automated installations will be transmitted (use control);
- 5) to guarantee that persons authorized for the use of a data processing system shall have access through automated installations exclusively to personal data which are subject to the accessibility authorization (access control);
- 6) to guarantee the possibility to investigate and establish to which agencies personal data can be transmitted through automated installations (transmittal control);
- 7) to guarantee the possibility to subsequently investigate and establish which personal data were put into the data processing system, at what time, and by whom (input control);
- 8) to guarantee that personal data which are processed upon request will be processed only in accordance with the instructions of the requester (request control);
- 9) to guarantee that in the course of transmittal of personal data, as well as in the transportation of the respective storage media, these (data) cannot be read, altered or deleted without authorization (transport control);
- 10) to create the organization within a (respective) authority or industry in such a manner that it (such organization) will meet the special requirements for data protection (organization control).

concerning the regulation of personal information collection indicates that some attention has been given to problems at that stage, the primary focus of the American Act is regulation of the handling of data once they are in agency hands.

The basic unit of personal data in the Privacy Act is a "record." A record is defined as:

... any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history, and that contains his name or his identifying number symbol, or other identifying particular assigned to the individual such as a finger or voice print or a photograph. 126

In the operational sections of the Privacy Act, however, duties are imposed on agencies with respect to "systems of records." A "system of records" is defined thus:

... a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. (emphasis added) 127

As agencies are required to comply with the Act insofar as they maintain a system of records, the more limited definitions affect the information holdings of the agencies. The "system of records" definition uses the criterion of retrieval by identifier; the broader "record" definition includes information simply containing an

126 5 U.S.C. 552a(a) (4).

127 5 U.S.C. 552a(a) (5).

identifier. Further, the identifier is more broadly defined for "records" than for "systems of records."

The PPSC report makes a telling criticism of the Act and the discrepancy between "records" and "systems of records":

Where the Act fails to meet its objectives, the failure can often be traced, in part, to the record and system of records definition that further limits its scope of application ... Unless an agency, in fact, retrieves recorded information by reference to a "name ... identifying symbol, or other identifying particular ...," the system in which the information is maintained is not covered by the Act. Whereas the record definition refers to information about an individual that contains his name or identifier, the system of records definition refers to information about an individual that is retrieved by name, identifier or identifying particular. The crucial difference between the two definitions is obvious, and the effect has been to exclude many records from the Act's requirement that are not accessed by name, identifier or assigned particular. 128

A related criticism of the scheme illustrates the relative novelty of automated filing systems. The PPSC says:

A further and extraordinarily important flaw in the system of records definition is that it springs from a manual rather than a computer-based model of information processing. In a manual record-keeping system, records are apt to be stored and retrieved by reference to a unique identifier. This, however, is not necessary in a modern computer-based system that permits attribute searches. 129

Thus, although the American scheme relies on the informed individual to keep a check on the personal information holdings of federal

128 Appendix 4, 5.

129 Appendix 4, 6.

agencies, there are some definitional problems which hamper the operation of the scheme.

For records contained within a "system of records," the Act creates an elaborate scheme affecting transfers of records and providing for subject access and correction of records.

Subsection (b) of section 552a, entitled "Records maintained on individuals," sets forth a general principle requiring non-disclosure of records by agencies. Agencies are not to disclose records without prior consent or written request by the individual. Eleven exceptions to this general rule are then listed. The first three of these do much to undermine the effectiveness of the protection suggested by the general rule. First, officers and employees of the agency "who have a need for the record in the performance of their duties," may obtain the record.¹³⁰ Second, the individual need not be consulted before records are released pursuant to the Freedom of Information Act.¹³¹ Third, if disclosure is "for a purpose which is compatible with the purpose for which [the record] was collected," the general rule is waived. Known as "routine use," transfers for this purpose are exempt from the disclosure rule of section 552a(b).¹³² Another important exception allows disclosure for criminal or civil law

130 5 U.S.C. s. 552a(b) (1).

131 5 U.S.C. s. 552a(b) (2).

132 5 U.S.C. s. 552a(b) (3).

purposes without consent of the data subject.¹³³

Certain transfers of the record are subject to a requirement that an accounting of disclosures to third parties be maintained. The accounting indicates the "date, nature and purpose" of the disclosure, and the identity of the recipient.¹³⁴ It appears that the accounting is kept notwithstanding that consent to the transfer has been obtained from the data subject. No accounting is required for routine use or "freedom of information" transfers. The data subject may inspect the accounting, which is retained by the agency for "five years or the life of the record, whichever is longer."¹³⁵ All accountings, except those for transfers for law enforcement purposes, are open to the data subject.¹³⁶

Following such requirements creates an audit trail -- a procedure unique to this statute, and undoubtedly a more informative method of indicating file use than merely publishing descriptions of "routine use" (in the U.S.) or "derivative use" (in Canada). However, the effectiveness of the accounting method is substantially reduced by the fact that it does not include transfers for routine uses, which represent the majority of transfers. As a result, the accounting

133 5 U.S.C. s. 552a(b) (7) .

134 5 U.S.C. s. 552a(c) (1) (A) , (B) .

135 5 U.S.C. s. 552a(c) (2) .

136 5 U.S.C. s. 552a(c) (3) .

device has been criticized as one of the most costly provisions of the Act, and one least used by data subjects.¹³⁷

Subsection (d) provides access to and correction of the record by the data subject. As in the French statute, the statutory language prescribing the procedure for access is very detailed. Access to a person's "record or to any information pertaining to him" may be gained by the concerned individual upon request.¹³⁸ The data subject may be accompanied by someone chosen by the individual, and a copy of the record may be made "in a form comprehensible to him."

Unlike the Freedom of Information Act,¹³⁹ there is no time limit set for agency compliance with an access request. With respect to corrections desired by the data subject, the agency is under a duty to either make the requested correction or inform the data subject of its refusal, the reasons therefor, and the right of appeal.¹⁴⁰ A request for amendment must be acknowledged within 10 days, and a decision must be made "promptly."¹⁴¹ Where an agency does not satisfy the individual's request, a notation of the disagreement may be filed with

137 Appendix 4, 70.

138 5 U.S.C. s. 552a(d) (1).

139 5 U.S.C. s. 552(a) (6) (A) (i). This paragraph gives the agency 10 days from receipt of the request for access, to determine whether to comply.

140 5 U.S.C. s. 552a(d) (2).

141 5 U.S.C. s. 552a(d) (2).

the agency by the individual.¹⁴² A later subsection requires each agency to make further rules for the implementation of these duties.¹⁴³

All agencies may pass rules to exempt certain records from access by the data subject. These exemptions are contained in sections 3(j) and (k).

Records maintained by the Central Intelligence Agency and law enforcement agencies (including some court records which in Ontario would now be considered public records) may be exempt from most requirements of the Act. These agencies are not exempt, however, from the restrictions on disclosure and the requirements to account for disclosure, the requirement to publish notices in the Federal Register, the duty to maintain timeliness and accuracy, the duty not to maintain unauthorized records of exercise of First Amendment rights, the duty to establish rules to ensure security, and liability under the criminal penalties.

Subsection 3(k) allows seven additional categories of systems of records to be exempted from most of the Act's requirements. These are systems of records maintained in connection with law enforcement, investigations, statistics, testing material, and third party sources of information relating to government employees, contractors and military personnel. Although some compliance with the Act is still required,

142 5 U.S.C. s. 552a(d)(3).

143 5 U.S.C. s. 552a(f).

an agency exempting a system of records in this way

is excused from granting an individual access to records about himself; from revealing to the individual its accounting of the disclosures it makes or records about him, from publishing certain portions of the required annual notice on the system, and promulgating regulations establishing procedures by which the individual can see, copy and correct or amend a record about himself. 144

Again, the drafting of the section in terms of "systems of records" creates difficulty in that it permits the exemption of more records than would be necessary to protect the interest in question. Not every record in a system of records would contain offending information, yet the wording requires that the entire system be exempt.

System notices published in the Federal Register provide information which will assist an individual who wishes to know whether a record about him/her is maintained. The Federal Register contains an annual notice containing information about names and locations of systems, a description of the contents of the system, routine uses, procedures for access, and agency rules promulgated pursuant to section 552a(f).¹⁴⁵ The Federal Register lists systems of records which are defined, as indicated above, as those groupings of records which are retrieved by personal identifier. Thus, the individual will only be able to monitor the records maintained by government in such systems.

144 Appendix 4, 8.

145 5 U.S.C. s. 552a(e) (4).

e) Transfer, Subject Access and
Correction in Canada

The Canadian Human Rights Act, Part IV, states that it protects the privacy of individuals "to the greatest extent consistent with the public interest," by providing a "right of access to records containing personal information concerning them for any purpose including the purpose of ensuring accuracy and completeness."¹⁴⁶

The statutory elaboration of this entitlement in section 52 of the Act indicates an emphasis on regulating transfer and correction of records to achieve the goal of privacy protection. An individual may:

- 1) know how the record has been used since its creation, or the implementation of the Act;
- 2) examine the record;
- 3) request correction;
- 4) if the record-keeper will not correct the record, insist that a notation of the request for correction be made.

Accessible records under the section are limited to those records in the control of the government institution which identify an individual by name or otherwise allow "readily ascertainable" identification, and which are used by a government institution in a decision-making process relating directly to the individual.¹⁴⁷ Access to these records is

¹⁴⁶ Canadian Human Rights Act, S.C. 1976-77, c. 33, s. 52(1).

¹⁴⁷ The Canadian Human Rights Act defines "federal information bank," "administrative purpose," "personal information," and "record" in s. 49.

facilitated by the publication of an Index of Federal Information Banks.¹⁴⁸ Exemptions to the general principle of subject access and to the publication of information in the Index are effected through conferral in the Act of broad discretionary powers on Cabinet ministers to exempt either an entire information bank or a particular record or portion thereof from the general rules.¹⁴⁹ When disclosure of a particular record or portion thereof is refused on the basis of a ministerial decision, the grounds for refusal must be communicated to the individual.¹⁵⁰

The Act permits three different types of exemption from disclosure in derogation of the objectives stated in section 52. The most restrictive of these confers a discretion to refrain from publication in the Index¹⁵¹ of information relating to the information bank. Alternatively, information about the bank may be published in the Index but the government has a discretion to deny all access to records within it. Exemptions of these first two kinds, relating to entire data banks, are made on the recommendation of a minister subject to Cabinet approval. The grounds for both types of exemption include the "likelihood" of injuring international or federal-provincial relations,

148 Canadian Human Rights Act, S.C. 1976-77, c. 33, s. 51(1).

149 Ibid., s. 54.

150 Ibid., s. 52(4).

151 Ibid., s. 53.

national defence or security, or disclosing information relating to law enforcement or national security investigations. Finally, even though a bank may be generally open, a record or portion thereof may be exempted from access when a request is made for it.¹⁵² The discretion to exempt particular records or portions thereof is conferred directly on the minister. In addition to the grounds for exemption set out above, exemptions on a case-by-case basis may be made to preserve Cabinet confidences, to avoid disrupting the operations of penal institutions or "impeding the function" of a court of law or like body, to prevent invasion of the privacy of a third party, or to avoid the disclosure of legal advice or opinion given to government.

The Act places some restrictions on the transfer of records. This is achieved primarily through the concepts of "derivative" and "non-derivative" uses of records. The former is a use "consistent with the use for which [the record] was compiled."¹⁵³ The Index published by the Treasury Board must contain a description of derivative uses. In order to use a record otherwise, a government institution must seek the consent of the individual.¹⁵⁴ Consent is deemed, however, where notice of the intended non-derivative use is given to the individual in writing, and no response is received within a specified time period.¹⁵⁵

152 Ibid., s. 54.

153 Ibid., s. 49.

154 Ibid., s. 52(2)

155 Ibid., s. 52(3).

The other limitation on transfer reiterates that personal information supplied to a provincial or federal authority in confidence may not be released under the Act.¹⁵⁶

The regulation-making power conferred by the Act on the Governor in Council enables the Cabinet to prescribe procedures for the implementation of the access and correction rights. The regulations may require the payment of fees. As a result, presumably, of the concern expressed in other jurisdictions that direct release of medical information to the concerned individual may be misinterpreted, or cause psychological harm,¹⁵⁷ special procedures may be devised "with regard to examination of medical records of an individual."

Although section 52 states that an individual is entitled to "ascertain the uses" of records subject to the Act, it appears from the Act that the only method of obtaining this information is by means of the listing of derivative uses in the Index. No provision for an accounting of disclosures, as is found in the American Act, is included in the Canadian statute. The extent to which these uses may be ascertained from the Index only extends, of course, back to the date on which the Act came into force.¹⁵⁸

156 Ibid., s. 50(2).

157 Ibid., s. 62.

158 Ibid., s. 52(1)(b).

4. Enforcement and Administration

The administrative machinery established by the data privacy statutes examined in this chapter have been alluded to but not specifically examined. Similarly, there have been isolated references to enforcement mechanisms, but no focus on them. In this section we will devote some attention to the apparatus with which each statute attempts to carry the privacy protection principles into action.

F.W. Hondius classifies mechanisms for the implementation of privacy statutes as falling into two categories; external controls and internal controls.¹⁵⁹ The external controls are imposed by institutions which are, for the most part, creatures established by the privacy laws themselves; i.e. Swedish Data Inspection Board, German Federal Commissioners, French National Commission on Data Processing and Liberties. The internal controls relate to "in-house" supervision of the security and quality of stored data, and are often implemented by already-existing bodies, such as the Treasury Board in Canada, and various executive branch agencies in the United States.

Hondius divides external controls into two sub-groups; subjective and objective. The first group is made operative by the person whose data is stored; the second requires some tribunal or board to survey the operation of the statute. Hondius offers three reasons for concluding

159 Hondius, op. cit., 209.

that controls cannot suffice in and of themselves to assure proper functioning of a privacy statute:

- 1) The data subject will have a biased and narrow perspective as to how the scheme should work;
- 2) The participation of data subjects will be sporadic and this may not be sufficient to exert consistent control;
- 3) "Differences of interpretation or appreciation" may arise between data bank and data subject requiring intervention of adjudication by a third party. 160

As will be seen, the role of subjective and objective mechanisms and their institutional structure varies dramatically from one jurisdiction to another. The American Privacy Act is a scheme whose effective operations depends to a considerable extent on enforcement initiatives undertaken by data subjects; there is no supervisory body for the implementation across all agencies, but rather an appeal of agency decisions to the court. Similarly, the German scheme offers little regulatory control. It may be described as a "mere" registration system, in that data operations need not be licensed but merely need to register their existence with the central agency. In other jurisdictions, notably Sweden with its Data Protection Board and France with the National Commission on Data Processing and Liberties, the final decision-making power over the implementation by record-keepers of the statute has been conferred on an independent regulatory agency. The French Commission has 17 members, some of whom are elected officials. There is thus a political component in its composition

160 Hondius, op. cit., 216.

which likens it to the New South Wales Privacy Committee. This political link and the tacit acknowledgement of the political dimensions of the responsibilities assumed by these bodies distinguishes it from the judicial nature of the ultimate controlling body for the U.S. Privacy Act -- the court. In Canada, the element of political control has been fully embraced as ultimate supervision is conferred on the ministers of the Crown. A federal appointee ombudsman has a "complaint" jurisdiction involving only advisory powers.

This examination of enforcement and administrative mechanisms will consider the internal or external nature of administration and its subjective or objective character, the composition of any external body vested with control powers, and the nature and extent of sanctions for enforcement.

a) Enforcement and Administration
in Sweden

The Swedish scheme lays great responsibility for proper data management on internal control, but relies on an independent administrative board to make broad policy decisions about the processing of personal information by the private sector. The Data Inspection Board is responsible for granting permission to operate a "register of persons."¹⁶¹

161 Swedish Data Bank Statute, s. 2.

Upon granting permission, the Board sets regulations according to which the registrar-accountable must run the register.¹⁶² Once established, the duties in upholding the operation of a register of persons without unduly encroaching on the privacy of individuals, and within the regulations set by the Data Inspection Board, fall largely on the registrar-accountable.¹⁶³ "The Data Inspection Board consists of a chairman, who may decide matters of lesser importance by himself, and eight other members," according to one account.¹⁶⁴ Their appointment is not, however, contemplated in the statute.

The supervision of the registers lies with the Board. It may change the regulations under which a register operates, or revoke the permission to operate a register. The broad rubric for changing regulations or revoking a permission is the "undue encroachment of privacy."¹⁶⁵

An appeal may be taken from any decision of the Data Inspection Board to the King in Council. In such cases, the Attorney General may represent the public interest.¹⁶⁶

162 Ibid., s. 1.

163 Ibid., ss. 8-14.

164 Selected Foreign National Data Protection Laws and Bills, op. cit., 65.

165 Swedish Data Bank Statute, ss. 3, 5, 6.

166 Ibid., s. 25.

A variety of sanctions are imposed by the Act for breach of duty. A register of persons established without permission may be "declared as forfeited."¹⁶⁷ The maintenance of incorrect information in a register may result in damages being payable by the registrar-accountable to the data subject.¹⁶⁸ Denial of access to the Data Inspection Board to premises where a data register is kept, or denial of requests for information from the Board may result in fines assessed against the registrar-accountable by the Board.¹⁶⁹ Similarly, a fine may be assessed by the Board for breach of other duties by the registrar-accountable.

The Act also establishes general offences which pertain to the following matters: the unlawful establishment or operation of a register of persons; the violation of a regulation promulgated for the operation of a register; the unlawful release of personal information; the delivery of incorrect information either to a data subject or to the Data Inspection Board; and the release of personal information or professional or business secrets, knowledge of which is gained through dealing with a personal register.¹⁷⁰

Persons convicted of such offences are subject to a fine or a term of imprisonment not to exceed one year. The amount of the fine is not

167 Ibid., s. 22.

168 Ibid., s. 23.

169 Ibid., s. 24.

170 Ibid., s. 20.

limited by the statute. The Act further provides that proceedings shall be instituted by the public prosecutor only where the aggrieved person requests it, or when the public interest calls for it.

A further and more serious offence of "data trespass," i.e. the effecting of unauthorized access or the making of improper alterations, deletions or additions to the records held in the register, is established by the Act. The penalty upon conviction may be a fine or imprisonment not exceeding two years.¹⁷¹

In short, the primary administrative mechanisms for the implementation of the Swedish Data Bank Statute are the two statutory creatures -- the Data Inspection Board, and the registrar-accountable. In Hondius' terms, the former falls within the "external control" category and the latter, "internal controls." Both are devised expressly for the purposes of the scheme, although to different ends. Matters of policy are assigned to the Board. The sanctioning provisions of the Act give the Data Inspection Board the power to penalize the registrar-accountable if the latter is not complying with certain of its statutory duties. The ultimate appeal body for decisions taken by the Board under the Act is political -- the King in Council. Added to this, as we have seen, is a comprehensive code of civil and criminal liability for prohibited practices relating to the operation of personal registers.

171 Ibid., s. 21.

b) Enforcement and Administration
in France

In France, the primary responsibility for the implementation of principles embodied by the data processing act (the Law Concerning Data Processing, Files and Liberties), does not rest on persons about whom data is stored. The National Commission on Data Processing and Liberties plays an active role in both administration and enforcement. It is involved from the inception of a data processing operation, at which point it issues decisions permitting the operation of data processing.¹⁷² It publishes a listing of data processing operations,¹⁷³ processes petitions for correction of files exempt from access,¹⁷⁴ and adjudicates claims that nominative data are being collected, stored or processed improperly.¹⁷⁵ Where appropriate, the Commission may recommend to the public prosecutor that infractions be dealt with by the court.¹⁷⁶ The Commission must also devise regulations to ensure security of data processing operations, and keep itself informed of developments in the data processing industry.¹⁷⁷

172 French Data Act, articles 14-17.

173 Ibid., article 22.

174 Ibid., article 39.

175 Ibid., article 26

176 Ibid., article 21(4).

177 Ibid., article 21(7).

The Commission is composed of 17 members appointed "for five years or for the length of their term of office."¹⁷⁸ It includes elected representatives from the National Assembly and Senate members. Their duties correspond to "external objective" controls, in Hondius' terms, in that the Commissioners have no direct ongoing interest in data regulation either as data subjects or data-keepers. Their responsibilities start with the mandatory authorization of data processing operations and extend to the setting of regulations for security measures, and overseeing them. In this latter role, the Commissioners ensure the proper functioning of internal controls on data operations required by their initial decree. The "subjective" control exerted by data subjects through their access and correction rights is also managed by the Commission. Articles 35 and 39 empower the Commission to allow a data processor to abrogate the data subject's right of access if requests can be characterized as nuisance, or if law enforcement or security reasons weigh against disclosure. Article 38 gives the Commission discretion in requiring a data processor to communicate corrections in data holdings to prior third party recipients.

There are four offences under the Act:

- a) causing personal data to be processed without the required declaration or Commission decision;¹⁷⁹

¹⁷⁸ Ibid., article 8.

¹⁷⁹ Ibid., article 41.

- b) unauthorized disclosure of information adverse to a data subject by intention or negligence; 180
- c) diversion of data from its proper destination; 181
- d) other violations of the present law:
 - . gathering data by fraudulent, unfair or illicit means;
 - . denying data subjects the right to contest that relevant data be subject to data processing;
 - . maintaining data beyond permissible time limits;
 - . failing to take proper security precautions;
 - . improperly gathering data on criminal matters;
 - . improperly storing religious, racial or similar personal data. 182

It is the duty of the Commission to relate information concerning these offences to the public prosecutor. Penalties range up to fines of two million francs (\$500,000) and five years imprisonment. The most serious offences are those involving the registration of improperly collected data, or data whose registration is forbidden by article 31.

c) Enforcement and Administration
in the Federal Republic of Germany

Compliance with the provisions of the German Federal Data Protection Act relating to public authorities is assured by the appointment of a

180 Ibid., article 43.

181 Ibid., article 44.

182 Ibid., article 42.

Federal Commissioner for Data Protection. This is required by statute to be a full-time position.¹⁸³ The Commissioner's function is to "exercise control over the observance of provisions of the [data] law."¹⁸⁴ In order to do this, the Commissioner may be required to submit reports to the German Federal Diet.¹⁸⁵ The Commissioner has powers of inquiry and inspection of data processing operations of government authorities and agencies.¹⁸⁶ The Commissioner must publish a register of "automatically operated information storage systems in which personal data are stored," and make it available to the public.¹⁸⁷ The Commissioner also has a complaints function,¹⁸⁸ and may lodge complaints, where appropriate, against the public authorities of federally controlled corporations whose data processing operations are regulated by the Act.

In addition to these administrative functions, the Federal Data Commissioner is an appeal body. Section 21 provides that "anyone may turn to the Federal Commissioner if he believes that his rights were violated" What the powers of the Commissioner are in this situation is not stated, nor are procedures for the appeal set out.

183 Federal Data Protection Act, ss. 17, 18.

184 Ibid., s. 19(1).

185 Ibid., s. 19(2).

186 Ibid., s. 19(3).

187 Ibid., s. 19(4).

188 Ibid., s. 20.

The appeal is limited to matters arising in the context of data held by public authorities.

There are also internal controls created by the Act. Section 15 sets supervisory powers to be exercised by the highest official in the government agency or government-controlled corporation. For the two categories of private data processing operations, an agent must be appointed for supervisory duties. The highest official must maintain a record of the types of personal data operations which are conducted by the government authority. It is this official's responsibility to ensure that those involved in the personal data process are aware of their duties and rights. The highest authority also has a duty to oversee the "proper operation of the data processing programs."

The primary responsibility of the agents in private data operations is to ensure compliance with the law. Since the duties of the Federal Data Commissioner extend only to governmental operations, it is within the power of provincial authorities to appoint a similarly empowered "supervisory board" with respect to private operations. In January 1979, all but two West German provinces had adopted their own data control acts.¹⁸⁹ The German system relies greatly on internal control

189 As of January 1, 1979, seven of eleven West German "Länder" had passed data protection laws:

Bavaria: April 28, 1978
West Berlin: July 21, 1978
Lower Saxony: May 26, 1978
Hessen: 1970, as amended January, 1978
Saarland: July 10, 1978
Bremen: December, 1977
Schleswig Holstein: June 1, 1978.

through voluntary compliance overseen by supervisory bodies. The duties of the "highest authority" and the Federal Commissioner do not intrude greatly on the operation of government personal data processing; they consist of supervisory functions with no strict procedures or sanctions to back them up. However, criminal offences punishable by imprisonment or fine are created for unauthorized transmittal, alteration, retrieval or procurement of personal data, with greater penalty if the acts are committed for the purpose of gaining profit or harming another.¹⁹⁰ There are also penalties set for violation of regulations; the failure to notify a data subject of stored data and various offences with respect to private data operations are punishable by fines of up to 50,000 marks.¹⁹¹

d) Enforcement and Administration
in the United States of America

In the U.S., administration of the Privacy Act is chiefly in the hands of each agency conducting personal data operations. Enforcement is effected through the courts for violation of the Act or regulations. The enforcement mechanism has been described by some as one of "self-help," for the burden of ensuring compliance with the Act lies with the data subject in correcting data and in bringing civil actions

190 Federal Data Protection Act, s. 41.

191 Ibid., s. 42. The value in Canadian dollars of 50,000 Deutschmarks (as of July, 1979) is approximately \$32,000.

for breach of an agency's statutory duties. The Act places obligations on the agencies to maintain records used in making determinations about individuals "with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual in the determination." The Act also requires agencies to take appropriate measures to ensure the security and integrity of records.¹⁹²

The absence of a statutorily designated custodian or supervisor with substantial responsibility for implementation of the Act distinguishes the American scheme from European acts examined previously. Each agency maintaining systems of records must comply with certain requirements,¹⁹³ and must pass rules to implement the requirements.¹⁹⁴ The Federal Register listing of these systems allows citizens to assure the accuracy and proper use of records kept about them. No external body is charged with the supervision of the whole scheme, nor is there a functionary within the agency appointed for this purpose. A study body, the Privacy Protection Study Commission, was established by the Act but was assigned the limited task of carrying out studies relating to privacy protection issues rather than overseeing implementation of the Act. The Act does provide, however, that the Office of Management and Budget, an executive agency, shall develop guidelines for the implementation of the Act and shall provide continuing assistance to

192 Appendix 4, 95-96.

193 5 U.S.C. s. 552a(e).

194 5 U.S.C. s. 552a(f).

the agencies and oversight of their efforts.

The case for appointment of a responsible individual was made by the PPSC. It found that implementation of the somewhat general data maintenance provisions of the Privacy Act worked where the agency used "formal structured approaches and mechanisms." It recommended:

In order to provide for more effective implementation of the Act, the Commission believes that the head of each agency should designate one official with authority to oversee implementation of the Act. 195

Against this background, the civil and criminal liabilities imposed by the Act must be seen as important means of ensuring agency compliance with the Act. Civil liability is imposed in a variety of situations. Where an agency refuses to amend the record as requested, refuses to comply with a request for access, fails to maintain records properly, or violates any rules or regulations resulting in an "adverse affect on an individual,"¹⁹⁶ the individual is granted a civil cause of action against the agency. Costs may be awarded to a plaintiff who has "substantially prevailed" in the action.¹⁹⁷

The criminal penalties established by the Privacy Act deal with wrongful disclosure by agency employees of agency records about individuals.¹⁹⁸

195 Appendix 4, 97.

196 5 U.S.C. s. 552a(g) (1) (D) .

197 5 U.S.C. s. 552a(g) (2) (b) , (3) (b) .

198 5 U.S.C. s. 552a(i) (1) .

Failure to comply with the system notice requirements of the Act is also an offence for agency employees.¹⁹⁹ It would appear that for these two offences, the officer or employee of the agency is personally liable to pay the fine which may be imposed. A third offence created by the Act prohibits the wrongful requesting of a file by anyone.²⁰⁰ In the case of each offence, a maximum fine of \$5,000 may be imposed.

It is interesting to note that the PPSC study suggests that in the American context, the offence provisions of the Act have proved to be something of a mixed blessing. The absence of an independent body to oversee implementation of the Act combined with the widely known (among agency personnel) presence of criminal penalties for wrongful disclosure of data results "too often" in the withholding of information upon application for access. The PPSC argues that a formal and structured approach to the implementation question is necessary:

Those agencies that have established formal structured approaches and mechanisms to implement the Privacy Act are the most successful in their implementation of the Act. ²⁰¹

According to the PPSC, "Someone other than the individual record subject must be in a position to hold agency record-keepers accountable; the Act's individual enforcement model is simply ineffective on a broad scale."²⁰²

199 5 U.S.C. s. 552a(i) (2) .

200 5 U.S.C. s. 552a(i) (3) .

201 Appendix 4, 97.

202 Ibid.

e) Enforcement and Administration
in Canada

Like the American Act, the major vehicle for external control of the implementation of privacy protection policy established by the Canadian Human Rights Act, Part IV, depends on the initiative of data subjects in taking steps to gain access to and correct records. There is no statutory requirement of registration or approval before data banks are established, nor is there any external instrumentality established by the Act which can require the data-keeper to comply with the principles of data protection set forth in the statute.

The exercise of access and correction rights is obviously facilitated by statutorily required publication of the Index to Federal Information Banks. The procedures for implementation of these rights are not prescribed by the Act, however, but can be set forth in regulations promulgated under the Act. Determinations with respect to the information which is to be exempt from access are made by the Cabinet minister responsible for the government institution holding the record.²⁰³

The closest approximation to external control to be found in the Canadian Act resides in the role assigned to the Privacy Commissioner. Essentially, the Privacy Commissioner's jurisdiction is to investigate complaints made by anyone alleging that rights conferred by the

203 Canadian Human Rights Act, S.C. 1976-77, c. 33, ss. 53, 54.

legislation have been denied.²⁰⁴ No one has the right to a hearing in connection with an investigation, but if the Commissioner comes to the conclusion that a right has not been properly accorded to a data subject, a report of these findings may be made to the minister responsible for the government institution in question, together with a recommendation for action. Additionally, the Commissioner may carry out studies referred to her by the Minister of Justice, to extend protection of privacy beyond the range of government institutions covered by the Act.²⁰⁵ The Privacy Commissioner does not, however, have a statutory mandate to carry out independent investigations for the general purpose of ensuring that the policies advanced by the Act are, in fact, implemented by the agencies of government.

The Act does not create civil or criminal liability for breaches of the duties imposed by the Act. Not one of the rights or duties created by the statute is enforceable by the imposition of a penalty for non-compliance. One whose rights are denied under the Act must rely on the investigation of the Privacy Commissioner. Further, there is no avenue for challenging a ministerial classification of certain personal information as exempt from access. Clearly, the success of the Act depends greatly on the good faith and sensitivity to privacy concerns on the part of government officials and employees.

204 Ibid., s. 58(1), (2), (3).

205 Ibid., s. 58(4), (5).

The Act does, however, provide for internal oversight of agency conduct by imposing duties of supervision on a member of Cabinet. Various administrative and supervisory tasks are assigned in the Act to the "designated minister." These have in fact been assigned to the Treasury Board.²⁰⁶ Thus the Board has assumed responsibility for publishing the Index, for performing an ongoing review of compliance with the Act, and for approving the establishment of new information banks.²⁰⁷ An elaborate set of guidelines for the design and approval of information banks, the handling of subject access and transfer requests and for the maintenance of records concerning data banks were added to the Treasury Board Administrative Policy Manual in December, 1978.²⁰⁸ The evident inadequacies of citizen initiative and the merely advisory powers of the Privacy Commissioner as instruments of supervisory control may be compensated for by a vigorous attention, on the part of the Treasury Board, to the privacy protection implications of its administrative supervision of government information practices. It is not yet clear, however, that internal administrative supervision will gain broad acceptance as a privacy protection mechanism sufficiently immune from concerns of cost reduction and administrative expediency.

206 Ibid., Statutory Instrument 78-33 appoints the Treasury Board as the "designated minister" under the Act.

207 Canadian Human Rights Act, S.C. 1976-77, c. 33, s. 56.

208 Treasury Board Canada, Administrative Policy Manual, c. 410, 415, 420, 425 (1978).

D. Conclusions

At the risk of gross oversimplification, we might identify three broad areas of concern addressed by the privacy protection legislation briefly reviewed in this chapter. The first affects collection of data and the setting up of data banks. What data may be collected? Under what terms and conditions should it be gathered and held? The second is concerned with data management. Once personal information is given to a government or other agency, who may obtain it from the agency? For what purposes will it be used? How long can it be retained before going "stale"? A right of access and correction for the data subject is the specific aspect of data transfer which is dealt with by most of these statutes. Finally, attention must be drawn to the mechanisms for administration and enforcement of the scheme.

In some of the European jurisdictions, privacy legislation deals most rigorously with all three aspects of data regulation. In Sweden and France, as a result perhaps of the initial impetus of concern with the use of computers, attempts have been made to regulate the entire process of personal data handling. The collection of personal data is limited to certain types of information, and the creation of data processing operations is closely monitored by an administrative body whose sole purpose is to administer the data regulation scheme. The German scheme, as we have seen, is more modest. The Federal Data Commission in Germany is also required to oversee public data banks, but the

setting up of the operations is not regulated by statute. The only stipulation on information collection is that the data subject consent to it, or that a statute permit it.

Although the American and Canadian schemes approach the subject of data collection less vigorously than the European schemes, it is clear that a consensus is emerging that the voracious appetite of government agencies for data collection poses a threat to privacy values and should be brought under some form of internal or external control. In the United States, agencies are required to gather and maintain information according to certain statutory standards which are elaborated by agency-promulgated rules. The Canadian Human Rights Act stipulates similar objectives for the government data management process. Records of personal information maintained by government should be accurate and complete. Unnecessary collection is to be eliminated. For the most part, however, realization of these objectives is placed in the hands of the internal financial management agencies; the Office of Management and Budget in Washington, and the Treasury Board in Ottawa.

The data regulation schemes examined here also offer evidence of an emerging consensus with respect to general principles of privacy protection in the context of data management. Transfers of data to third parties should be brought under control, whether by the prohibition of some kinds of transfers, the requirement of notice of possible transfers at the time of initial collection, the requirement

of the data subject's consent, the requirement of the approval of a regulatory agency for particular kinds of transfers, or some combination of these methods.

Further, the principle of allowing access by the concerned individuals to personal data files in order to learn what information about them is being maintained, and to assure the accuracy of that information, has been accepted in all five jurisdictions. The specificity with which this right is set out in the legislation varies widely, as does the extent of access. The same may be said of the right of correction. The German statute simply provides, "personal data shall be corrected if they are wrong," while the American text runs longer than a page with precise detail as to the nature and exercise of that right.

Four of the five jurisdictions examined accept the value of publicity, with respect to the existence of personal information data banks, as an important instrument for privacy protection. In Germany and France, the Index appears designed simply to assist data subjects in locating records which might contain information concerning themselves. In the United States and Canada, some reliance is placed on the publication of the Index as a device for encouraging less intrusive data management practices.

Although there is also evidence of a consensus concerning the need for administrative and enforcement machinery in each of the jurisdictions examined, the mechanisms employed vary considerably in their

institutional structure and in the extent and nature of the powers conferred upon them. In each jurisdiction, the administration and enforcement schemes include an "external" official person or body of officials especially appointed to administer or oversee the implementation of the privacy protection principles. The degree of activity authorized and the extent of the authority wielded ranges from the limited role of the Privacy Commissioner in Canada to the comprehensive powers of the French National Commission on Data Processing and Liberties, whose duties extend from approving personal data operations to investigating complaints and recommending prosecutions for infractions of the law. Of all the jurisdictions considered, the mechanisms of administration and enforcement in the Canadian scheme are the least powerful and the most "internalized."

Further, in all jurisdictions but Canada, some role for the imposition of criminal sanctions has been deemed appropriate. Whether the Canadian approach manifests a sophisticated philosophy of restraint in the use of the criminal sanction rather than a naive faith in human nature or a failure to recognize the need to consider the various pressures which conduce to more invasive administrative practices, is a matter yet to be determined.

The concepts of data protection and the individual's right of access to personal information held by government or other large processing operations have been accorded substantial recognition in the jurisdictions under examination here. Clearly, there are important

choices to be made in determining the extent to which privacy protection principles shall extend into data processing operations, and how a data protection scheme should be enforced. Our survey suggests that to simply enact legislation creating a cause of action for invasion of privacy, as in Manitoba, Saskatchewan and British Columbia, does not meet the problems which are included in the notion of informational privacy. The non-regulatory approach taken in New South Wales is appealing to the extent that it tests carefully the need for new regulation in the protection of "privacy" interests. However, many jurisdictions have apparently reached the conclusion that stronger measures are necessary to meet the threat to privacy posed by modern information gathering and handling practices.

CHAPTER VII

CONCLUSIONS AND RECOMMENDATIONS TO THE COMMISSION

A. General Conclusions

1) Personal records kept by government have grown rapidly in number and detail. Table 1 on the following page gives an indication of the scope and extent of personal record-keeping by the Ontario government. These collections of records about people have been accumulated as a direct result of the increasing number of activities in which government has become involved since the Ontario legislature was established. They have closely paralleled the growth of personal record collections by almost every other contemporary Western democracy. Nearly every new service provided by government or regulatory power granted to government has meant the creation of yet another set of records about the individuals or organizations for whom the service was intended or whose lives or businesses were to be regulated (see Table 2). As we pointed out in Chapter II, the growth of records held by government has been an essential and often unwitting administrative by-product of each separate decision to extend the ambit of government operations. Concerns for privacy have arrived late on the scene, at a time when government records already touch almost every aspect of our

TABLE VII.1

SOME OF THE PEOPLE ON WHOM THE
ONTARIO GOVERNMENT KEEPS PERSONAL RECORDS

AGRICULTURE AND FOOD

Farmers (cattlemen, dairymen,
cash crop growers, etc.)

ATTORNEY GENERAL

Persons involved in criminal
and civil court cases

CIVIL SERVICE COMMISSION

Ontario government employees,
past and present
Applications for government jobs

COLLEGES AND UNIVERSITIES

University students
Certified tradesmen
Apprentices
Community college applicants
Student nurses

COMMUNITY AND SOCIAL SERVICES

Municipal Welfare recipients
Family Benefit recipients
Senior citizens
Adopted children and
adoptive parents
Disabled persons
Children's Aid wards
Juveniles in Training Schools
Mentally retarded persons

CONSUMER AND COMMERCIAL

Births, marriages and deaths
Real estate, car and
travel salespersons
Creditors and debtors

CORRECTIONAL SERVICES

Persons accused and convicted
of criminal offences

EDUCATION

Teachers
Grade XIII students

HEALTH

Physicians and surgeons
Nurses
Hospital and doctors' patients
Victims of contagious diseases
Patients receiving special care

HOUSING

Public housing residents
Ontario Housing mortgagees
Senior citizens

INDUSTRY AND TOURISM

Businessmen
Tourist establishment operators

NATURAL RESOURCES

Commercial fishermen
Hunters and anglers
Park users

REVENUE

Guaranteed Annual Income
Supplement recipients
Property owners
Taxpayers

SOLICITOR GENERAL

Deceased persons
Victims, witnesses, suspects
and convicted persons
Government employees with
security clearance
Private investigators and
security guards
Owners of firearms

TRANSPORTATION AND COMMUNICATIONS

Licensed drivers
Vehicle owners
Traffic accident victims

TEIGA

Tax reductions for farmers
and for senior citizens

TABLE VII.2

SOME MILESTONES IN THE GROWTH
OF ONTARIO GOVERNMENT SERVICES

| | |
|------|---|
| 1958 | General Welfare Assistance Act Ontario Scholarships |
| 1959 | Hospital Insurance |
| 1961 | Elderly Persons Social and Recreational Act |
| 1963 | Ontario Graduate Student Fellowships |
| 1964 | Department of University Affairs created Ontario Housing Corporation |
| 1965 | Colleges of Applied Arts and Technology created Children's Services extended under Child Welfare Act |
| 1966 | Legal Aid introduced Ontario Medical Services Insurance Plan |
| 1967 | Home Ownership Made Easy Mortgages |
| 1967 | Ontario Development Corporation created |
| 1972 | Ontario Health Insurance Plan |
| 1972 | Committee on Government Productivity - general reorganization of the Ontario Government |

Source: Vernon Lang, The Service State Emerges in Ontario
(Ontario Economic Council, 1974).

lives. The current emphasis on reducing government spending will mean that the creation of large programs in new areas of government activity is likely to be less frequent than in the past. However, there are indications that the same trend towards reduced government spending may lead to more extensive collection of information about people, particularly where eligibility and need for service is subject to increasingly rigorous tests. We note, for example, the recently instituted requirements for Ontario Student Award applicants to give approval for the Ministry of Colleges and Universities to have access to their income tax records. In addition, as government tries to improve the effectiveness of its programs or to identify new areas of activity, more use will be made of personal records in planning and research.

2) While the assessment of Ontario government record-keeping practices found that far too much information about individuals is collected and kept by provincial agencies, and that lack of policy and careless habits have in several areas created the potential for privacy invasion, it concluded that the privacy of citizens has as yet not been intentionally abused by government information handling practices. There are no all-encompassing dossiers from which some mysterious force is extracting information with which to rule private lives. Citizens may feel at times that the forms they fill in are tedious and unnecessary, and they may wonder what happens to the information they provide, but as a general matter, Ontario residents can expect to be educated, to be granted credit

and to own a house or drive a car without yielding many of their inner secrets, and without promoting privacy intrusive activities by government agencies.

3) It is when people cease to be healthy or self-supporting, or for one reason or another come to the attention of those involved with enforcing the law, that privacy may be jeopardized by giving up personal information to government. Insurance companies do attempt to verify health records; welfare officers do occasionally check car licence plates to see who is visiting whom; employers do sometimes check criminal records; the police do collect intelligence information about certain kinds of criminal or political groups.

In many cases there are quite understandable reasons behind these desires to collect personal information. Some people do try to defraud insurance companies; others try to cheat the welfare system; there are people whose past behaviour represents a definite risk in positions of trust; and some crimes are in fact committed by organized groups. The problem is how to determine the balance between an understandable need to know and the privacy of both the individuals concerned and others who contribute sensitive information to records held by government.

4) There is a growing use of computers in government. Most of the large record collections studied, including those pertaining to health, licensed drivers and vehicles, student loans, law enforcement,

corrections and income supplements are already computerized. In almost all the areas examined, major new computerization projects are under way or are in the process of being planned, and most agencies view the computer as one of the key elements in a drive towards greater efficiency and improved management effectiveness. Government currently lags behind the private sector in its use of computers, primarily because restraints on government spending in recent years have held back development. However, the move towards computerization and the use of advanced communications technology is inexorable. The effects of these technologies upon the privacy of Ontario citizens has neither been completely assessed nor fully considered in decision-making about automating record systems.

5) The impact of computerization on privacy can be both good and bad. The effect of computerization is usually to bring together information in a common format in one single location. This means that, although the technical expertise required to do so is sometimes highly specialized, it is possible for a person with access to the computer file to rapidly scan the entire file and to extract data from it. However, computerizing data enables greater physical security to be maintained and more foolproof techniques to be adopted limiting the accessibility of data. For example, it is possible to automatically log use of the data, and to suppress portions of the data which should not be revealed for reasons of confidentiality.

While, as yet, computers do not appear to have significantly contributed to invasions of privacy, our study indicates that their potential for doing so is very real. For example, a central data bank in which all the information is in a neat identical format can be a tempting resource for more than one potential user, and the possibility of combining data banks which together form a much more useful profile than they do separately can be attractive. The potential for integrating various types of personal data is enhanced by wide and increasing use of the Social Insurance Number as a personal identifier. The need for some controls over potential privacy invasion by computer is apparent.

Another danger of computerization is the fact that manually collected data must often be made amenable to automation, and therefore be reduced to a common format, usually a form of code. The quality, or detail of the original data is therefore diluted, and the dilution is often subject to the judgment of whoever is doing the coding. For example, an indication of "psychiatric problem" can cover anything from mild depression to severe psychosis. In the hands of someone who may be unaware of verification or documentation procedures, such information could obviously be harmful to the individual concerned. Computerization creates an additional potential for privacy invasion if knowledge, ethics or standards are lacking among professionals who regularly handle computers and computerized personal data. As an illustration of this problem, Dr. John Carroll of the University of Western Ontario discovered in surveys that computer science students have little regard for either

data subject privacy or rules protecting data from illicit use.¹

Finally, data communications which provide remote access to computer files create an obvious potential for breaches of confidentiality. With the dispersal of many government services across the province in regional and field offices, data communications as a means of both connecting and disseminating data has become more feasible. A number of ministries are investigating or have already implemented data communications systems.

B. Areas of Concern

Rather than focus on particular ministries which, based on the case studies chosen for in-depth study, appeared to experience more difficulties than others in handling privacy issues and personal record-keeping problems, our conclusions instead concentrate on five internationally recognized informational privacy concerns needing attention throughout government. These areas of concern are:

- . Public Knowledge of Data Banks
- . Collection of Personal Information
- . Maintenance and Security of Personal Information

1 Carroll, John, Lecture at University of Western Ontario, October 10, 1978, as quoted in "Universities teach illegal computer use, professor says," Globe and Mail, October 11, 1978. His findings are also examined in the monograph Prevention of Computer-Based Fraud (London, Ontario: University of Western Ontario, September 30, 1978).

- . Transfer and Dissemination of Personal Information
- . Subject Access to Personal Information.

1. Public Knowledge of Data Banks

1) There is no adequate overall listing or index of personal records held by the Ontario government, nor is there any regular reporting of developments in record-keeping and information systems. In an attempt to gain an understanding of the extent of record-keeping in the Ontario government, the study group examined listings of information systems and data banks from several sources, none of which provided a satisfactory basis for analysis. Some of the lists dealt only with computer systems; some dealt with records gathered for statistical purposes; and others were concerned with record series at a detailed "filing cabinet" level. Since none of these lists was compiled for the purposes of public information, it was not surprising that they generally failed to be satisfactory for this purpose. In the absence of an accurate, complete and regularly updated compilation, it is extremely difficult for record subjects to ascertain what and where information about them is kept, and for interested members of the public to evaluate government record-keeping practices. This problem is particularly serious in the law enforcement area where, in effect, secret data banks exist. The public has little, if any, knowledge of the types of intelligence and crime prevention activities in which

the police participate or the extent of information collected in the course of such activities.

It is clear, however, that there is sufficient information about most records kept by the various Ontario ministries and agencies for an overall index to be readily compiled. Most manual record collections have been scheduled as to their storage and eventual destruction, and the size of each record collection has been documented. In addition, an annual report is made to Management Board as part of the budget preparation process by each ministry concerning its computer systems currently operating, under development or planned.

2. Collection of Personal Information

2) Although there is a growing awareness of the privacy issue, considerations of privacy have rarely entered into decisions about information collection by government. The investigation of various government data banks revealed that personally sensitive information is routinely gathered by several ministries, including those dealing with health, education, employment, social services, law enforcement and corrections. Some potentially privacy-invasive methods of collecting information, such as the utilization of neighbours and relatives as information sources, were also discovered. Perhaps because privacy is such a value-laden issue, no forum for debate over privacy

and record-keeping concerns has been established until recently. Instead, administrators have been left on their own to make judgments about what to collect and what not to collect, except where data collection parameters are laid down specifically in statute or regulation. Decisions have therefore been based largely on the perceived need for information in the administration of a particular program. The overriding objective of a program may be such that those administering it may lose sight of privacy as a valid consideration in record-keeping decisions. This is especially the case both in the social services -- where the fact that people are being given help is often seen as justification for overlooking their privacy needs -- and in law enforcement -- where it is argued that the objective of protecting society should be paramount over rights to privacy. In recent years, the impact of specific methods and kinds of data collection on privacy -- most notably, electronic surveillance in the field of law enforcement -- has resulted in legislation to establish a balance between privacy and society's need to know, but the vast majority of information collection activities by government are unimpeded by any forced concern for privacy.

3. Maintenance and Security

3) Policies regarding retention and destruction of personal data have either been absent or inconsistently applied at the service delivery

level. The quality of personal information often deteriorates over time, especially when it is automated. Although the Manual of Administration issues guidelines on the subject, and all ministries utilize retention schedules for records management purposes, neither the guidelines nor the retention practices are based on privacy considerations. To our knowledge, no provincial program regularly destroys client records shortly after client service terminates in order to avoid the utilization of that record for "labelling" purposes. How personal records are to be destroyed is another unsettled question in the Ontario government. The potential for privacy invasion created by this policy gap is illustrated by testimony before the Krever Commission which revealed that the mishandling of medical files containing extremely sensitive patient information in transit to garbage dumps caused this material to be blown across city streets.

4) Technical system security is generally adequate, but personnel security practices often expose personal information to unauthorized use. A continuing awareness of the need for security must be maintained. There are no overall standards for security of personal records held by the Ontario government. Similarly there is no classification system for files or documents. However, the Manual of Administration does contain minimum standard practices for the security of operational computer systems and master files. A recent status check on systems integrity carried out by a consulting firm on behalf of the Management Board Secretariat concluded that security procedures for transaction

origination, data entry, data communications and computer processing are generally adequate. The study also concluded that system controls in the government data processing centre examined are as good or better than those employed by the average private sector computer centre. We did not conduct our own investigation to verify these findings.

However, computer and telecommunications technology are advancing with such rapidity that accessing and transferring data by both licit and illicit means becomes cheaper and easier almost every day. At the same time, few incentives exist for the government to improve data protection. Implementing technical security measures was seen by many interviewees as expensive and time-consuming.

Technical security measures such as checks on computer system integrity, various system protocols, locked computer and telecommunications access points, and encryption make up only one facet of the security problem. The study pointed out that unauthorized use of data by authorized personnel is the weakest point in the security armour surrounding personal data. Our own observations confirmed that high staff turnover and use of private consultants significantly contribute to the security problem. It also found that careless personnel practices -- such as leaving personal records in unlocked drawers and filing cabinets and open offices, taking records home, talking about clients over the telephone before checking the identity of the caller, and discussing client business in public areas -- were responsible for a number of security breaches.

Enhancing this problem is a lack of sophistication in many Ontario government computer systems, which require the performance of several manual tasks prior to information computerization, including copying information onto special forms, coding, keypunching, transporting to a computer facility, and inputting at a computer terminal. At each of these steps, personal records become less accurate and are more likely to be lost or misplaced. In fact, officials in various ministries reported to us that forms are often lost during these processes.

In considering the need for security, it is necessary to understand both the possible uses which could be made of personal information and its potential value to others. While many of the government's personal record collections would be of little use to anyone other than the program staff who gather it, other collections could be of sufficient value to encourage outsiders to take unusual steps to gain access. The present controversy over unauthorized access to medical records by insurance companies and employers is a case in point.

4. Transfer and Dissemination of Personal Information

5) The transfer of personal records among government record-holders is not controlled by consistent policy. Few government programs have formal policies to protect the confidentiality of the personal information which they collect. The majority of government officials interviewed

stated that personal information maintained by them is confidential, except where public disclosure is permitted by statute or tradition, but the definition of "confidential" varied considerably by interviewee. Moreover, the study group gained the impression that any protectiveness toward records was a result more of bureaucratic reserve than of any strong concern for individual privacy. We found several instances of regular formal data sharing between the data banks of different (non-related by policy field) programs. An obvious example is the direct access and use by the police of motor vehicle and driver information held by the Ministry of Transportation and Communications. Indeed, there is a considerable amount of information sharing by many non-justice programs with agencies in the justice field, and among justice agencies themselves. A great deal of data sharing also takes place among social agencies and between social service and non-social service programs, particularly by word-of-mouth, but also by formalized arrangements, such as the transfer of school attendance records about welfare recipients to welfare programs. A situation in which few policies dictate exactly when and to whom these transfers are appropriate increases the possibility for individual decisions (either knowingly or unknowingly) to violate the personal privacy of record subjects. The Ministry of Corrections is the only ministry studied which has formulated and implemented comprehensive rules regarding the transfer of personal information.

6) The most extensive sharing of sensitive information appears to take place in the social services. Apart from medical data, personal information collected by social services agencies is probably the most sensitive of any personal records collected by government. This sensitivity is due to the fact that reliance on social assistance, such as welfare, is seen by many to be a stigma, and to the fact that eligibility determinations often require ongoing surveillance of recipients' circumstances — whether they are looking for work, with whom they are living, what they are buying, etc. In an attempt to help clients, social service agencies frequently collect subjective information about attitude and behaviour — which may involve discussions about clients with employers, teachers and neighbours as well as information sharing with other ministries, such as Health and Education — often without the knowledge of the individual. There are some signs of a growing awareness of the need to consider the privacy of the individuals with whom social service agencies deal. The study group found the work being done in this area by the Children's Services Division of the Ministry of Community and Social Services to be most encouraging.

7) Breaches of confidentiality are most likely to occur at the day-to-day operating level. The greatest concerns for confidentiality were held by managerial staff. Most administrative and clerical staff were aware of the need for confidentiality; however, we found more informal sharing of information at the operating level, often by word of mouth,

among those with shared interests in a particular client group. The major controlling factor in the dissemination of personal information at this level is the fact that such sharing in general takes place only among members of what is perceived to be a "professional" group. Thus, social workers share information with educators or other public servants. Confidentiality is, therefore, partly preserved by a sense of "professional ethics," rather than by any formal policy, although many interviewees mentioned the oath of secrecy sworn by all civil servants. The inherent dangers in this situation are that both the appreciation of the need for physical security in personal record-handling and the qualifications for membership in the "professional" group authorized to receive sensitive information vary by individual record-handler. (One employee, questioned about the type of person who might fit the professional category, replied that anyone carrying a ministry identification card would be permitted access to sensitive records. Over 20,000 people in that ministry carry such a card.) Furthermore, because sharing information among "helping" professionals is considered in the best interests of the client, the record subject's need for prior knowledge of and consent to such transfers is frequently overlooked.

8) Notwithstanding the lack of controls over information sharing, the majority of government programs are quite distinct and separate from each other, leading to considerable duplication of information gathering and storage activities. The threat to privacy presented by this

situation is that the individual requesting a number of similar government services may be required to divulge very sensitive information several times to several government personnel. As one interviewee stated, there is a certain "territorial imperative" exercised over information which raises intrinsic barriers to data sharing, even where such sharing would clearly be advantageous to the client. In addressing this concern, government officials must be careful to avoid creating another problem conducive to privacy invasion -- over-integration of personal records among programs with dissimilar objectives; for example, rehabilitation and income maintenance programs.

9) In certain cases, the public interest in having access to personal records outweighs any privacy interest in suppressing them from public view. For three of the records systems held by Ontario government ministries which we examined -- the Driver and Vehicle files in the Ministry of Transportation and Communications and the Personal Property Security Registration System in the Ministry of Consumer and Commercial Relations -- record subjects may receive information from or may obtain a copy of their records. However, records in all three systems are also available to the public, raising questions as to whether or not the privacy of record subjects is thereby invaded. We concluded that the public interest in having access to these specific records outweighs any record subject privacy interests. On the other hand, we also concluded that lists of identifying information from driver or other government-held files should not be offered for sale except under very

controlled circumstances, and that record subjects should be notified and given the opportunity to control any potential record transfers at the time of information collection. Such situations highlight the tensions between freedom of information and privacy.

5. Subject Access

10) Most of the record collections examined are not accessible to the subjects of the records. Confidentiality often means that even the individual about whom the record is kept cannot gain access to it. While the majority of program personnel agreed with the idea of individual access, many had reservations about permitting access to the files for which they were specifically responsible. Few persons interviewed by the study group were aware of many actual requests received from individuals wishing to see their files; however, requests which had been received were usually denied.

Many rationales are cited for denial of subject access. In nearly all programs examined, files are regarded as being the property of the organization. The individual subject, therefore, is thought to have no rights regarding information contained in the record. Where subjective information or information gathered about the person from others is likely to be included in the file, this reluctance to reveal the contents of the file is particularly acute. Some record-keepers

fear record subject retaliation and civil suits. Also, many physicians and psychiatrists strongly resist any suggestion to share clinical information with their patients on grounds that open access to medical information may lead to misunderstandings and may be harmful to some patients. Many law enforcement officials believe that subject access must be restricted to avoid compromising third party sources or hampering law enforcement activities. Opening up access to personal records is foreseen by some to significantly affect information collection activities; it may, for example, encourage administrators to hide subjective judgments in private notebooks. Some predicted effects, such as more objective reporting of personal characteristics may, of course, be beneficial to record subjects.

At least one ministry has successfully implemented a broad subject access policy. Under section 231 of The Education Act, elementary and secondary school pupils and their parents are granted full subject access and correction rights to their Ontario Student Records stored at public schools. Despite a possibly adverse effect upon teacher record-keeping practices, the subject access provision appears to have been successful in allaying many parental and pupil fears about the contents and uses of their educational records. While the provision has not been widely utilized, we concluded that the availability of files in itself seems to reassure the public of the propriety of educational record-keeping.

C. Recommendations

1. Alternatives Examined

The alternatives we have examined are based upon what appear to be six distinct approaches to privacy and data protection taken in other jurisdictions, whether individually or in combination with one another. They were described in detail in chapter VI and are summarized below, together with a brief restatement of their pros and cons.

a) The Tort Approach

Legislation would establish a right to privacy, violation of which would be made actionable without proof of actual damage. This would provide individuals with a possibly expensive means of attempting to obtain redress through the courts, but would do little to solve the problems of data protection examined in this report.

b) The Data Regulation Approach

This approach would require data banks to be licensed and registered and to comply with certain standards regarding the collection, processing

and transfer of information. The requirement often applies only to automated record systems. We found, however, that in Ontario the most sensitive data is held in manual form and that unauthorized transfers of data are just as likely to occur in non-computerized areas. We therefore suggest that the computerized data regulation approach would only partially solve the privacy and data protection problem.

c) The Fair Information Practices Approach

Such legislation would provide mandatory individual access to records; require an accounting of non-routine uses or disclosures, allow for correction of errors in records, require that public notice of the records be given, and would provide civil remedies and criminal penalties for contraventions of the statute. Exemptions would be permitted for certain types of records. This approach meets all the criteria for a good data protection regime. However, there are concerns on the part of government officials that if it were imposed upon government agencies without adequate preparation, it could be costly, time-consuming and could result in considerable misunderstanding and frustration, particularly if applied immediately and instantaneously to all local government agencies as well as to the programs and agencies of Ontario ministries.

d) The Public Awareness/Ombudsman Approach

This approach would involve the establishment of a body whose purposes would be to examine and attempt to resolve complaints of privacy invasion, to carry out research on privacy issues and to heighten awareness of privacy concerns on the part of the public, the government, and the private sector. Given strong leadership, this approach could be very useful in laying the attitudinal and procedural groundwork for privacy protection, since it enables specific problem areas to be defined and focused upon. We would suggest, however, that this would only be useful as an important interim step toward clear legal safeguards for privacy. It is possible, however, that an interim period in which such an agency were permitted to operate effectively could reduce some of the initial costs of legislated rights to privacy protection.

e) The Freedom of Information Exemption Approach

It is conceivable though most unwise, in our opinion, to deal with the privacy problem by simply providing an exemption to any proposed freedom of information act whereby disclosure of personal information would constitute an invasion of privacy. The effect of such a provision would at least establish a standard for balancing freedom of information interests against privacy interests. We suggest, however, that the complexities of the privacy problem cannot adequately be addressed

through a mechanism of this kind. In the first place, a vague standard does little more than signal the importance of the question; it does not go very far in resolving it. Secondly, a freedom of information act -- since it must deal with the question of access by all citizens to all government files -- is not a satisfactory vehicle for dealing with the more limited question of an individual's access to files concerning him/her. As we have attempted to indicate, the access question is only one of many issues raised by the privacy question. In sum, then, the problem is not one to be solved as an afterthought to a freedom of information scheme.

f) Internal Administrative Guidelines

Finally, we examined the possibility of an internally administered data protection regime, through administrative guidelines and directives, which would include the principles embodied in a "code of fair information practice." A number of Ontario ministries are currently examining the practices and procedures governing privacy and should be encouraged to do so in a manner which is consistent throughout government. This approach would not have the public visibility of other schemes, but could assist in bringing about the required change in attitudes and practices necessary for a full data protection scheme to work.

Our suggestions to the Commission embody a number of the above approaches as a means of moving towards a full data protection scheme in a thoughtful and planned manner. It would be possible to consider only one of the suggestions independently of the others, but they are presented as a coherent set of measures to be taken together.

2. Goals and Objectives

In formulating our recommendations to the Commission concerning ways in which privacy and personal data might be better protected, we aimed at achieving five goals:

- . Improving public knowledge about government record-keeping
- . Providing a mechanism for complaints, research and debate about privacy issues
- . Encouraging government sensitivity toward record-keeping and privacy concerns
- . Providing record subject privacy rights
- . Balancing freedom of information and privacy interests.

a) Improving Public Knowledge about Government Record-Keeping

Improving public knowledge about personal records kept by government -- how and why records are collected; how they are processed, stored and destroyed; and the uses to which they are put, both within and among

agencies -- would involve the publication of an index to all personal data banks. This document would give an appreciation of the extent and nature of personal records kept by government and an indication of the uses made of the records. Jurisdictions where no index has been compiled have experienced little public interest in accessing files, and consequently a lack of interest in the subject of privacy has been demonstrated by their agencies. An index alone, however, has its limitations. It is a static document which gives no indication of trends in record-keeping, amalgamation or integration of record series, or technical innovations affecting dissemination of information from the files -- unless one compared different editions of the index over a period of time. More than any other cause, privacy concerns arise from the fear of potential uses and abuses of information, particularly where computers are concerned. A regular reporting of developments in personal record-keeping practices, in addition to a right of access, would do much to allay these fears. It would also provide a basis for informed discussion about privacy issues. Publication of government financial accounts is a mandatory requirement to inform the public about the use being made of the financial resources it provides. Since information, and particularly information about individuals, is an essential resource of government also provided by the public, a similar accounting should be provided.

b) Providing a Mechanism for Complaints,
Research and Debate about Privacy Issues

From our research and from comments made by our contacts in other jurisdictions, we have concluded that no privacy protection scheme would be effective without the establishment of a body to which citizens could complain about invasions of their privacy. Moreover, further research and debate on privacy issues would be essential to educate the public and government on these subjects.

c) Encouraging Government Sensitivity toward
Record-Keeping and Privacy Concerns

Our research revealed a need for government agencies at all levels to be encouraged to adopt a more sensitive stance towards privacy and confidentiality concerns. In addition, we found a need for staff to be more open with individuals about personal information held in government data banks. An increased awareness of privacy concerns among government agencies can be greatly encouraged by the formation of an independent body, which has both advisory and research roles, and which can deal with general complaints concerning government record-keeping practices. Such a body could also be instrumental in placing controls over information transfers and in setting record security and maintenance standards.

d) Providing Record Subjects Privacy Rights

The central theme of most data protection regimes is that the individuals about whom records are kept should be given the right to ensure that information about them is correct, and therefore should be able to have access to their files. The assumption is that the person most affected by information contained in the record would take whatever steps were necessary to see that the information was correct and adequately protected. Our discussions with persons involved in administering privacy legislation at the American federal level, in various states in the U.S., and at the Canadian federal level, indicate that with certain exceptions, public response to rights of access has been small. Although the right of access to personal files established by any of these jurisdictions aids in the resolution of misunderstandings and errors, it is unlikely that the typically small number of requests for access to files would force government agencies to develop a higher awareness of privacy considerations within these agencies. Although it is an important element in any data protection scheme, our research has led to the conclusion that individual access by itself is an inadequate solution to the need for data protection.

e) Balancing Freedom of Information
and Privacy Interests

We believe that freedom of information legislation will necessitate a

clearer definition of the boundary between freedom of information and privacy interests. Our discussions with persons involved in implementing privacy and freedom of information legislation in various American states and our review of reports on the U.S. Privacy Act and Freedom of Information Act confirm that there is a significant potential for conflict inherent in the purposes of the two types of legislation. Most jurisdictions have emphasized freedom of information over privacy, and exemptions to freedom of information provisions have therefore been narrowly interpreted. The public pressure for freedom of information legislation has been considerably stronger and more vocal than that relating to privacy legislation, as the proportion of briefs to this Commission attests. Briefs concerning freedom of information have outnumbered privacy briefs by a ratio of six to one.

The job of determining the balance between the individual's desire for privacy and society's right to know has in most cases been given to an appeals tribunal or directly to the courts, which have tended to favour disclosure. However, certain interests are beginning to be reaffirmed through "reverse freedom of information suits." This is particularly the case with commercial information, where competitive harm might result from the release of confidential information given by a company to a government agency. In addition, the first signs of the dangers of opening up law enforcement records were revealed recently by a witness before the U.S. Senate, who stated that he had used a Freedom of Information Act request to uncover and "deal with" informants, even

though the material given to him had been censored according to the exemptions available under the statute.

Although the concepts of privacy and freedom of information raise conflicting interests, both schemes do, of course, concern access to government files. The reasons for denying access in certain circumstances are, for the most part, common to both kinds of legislation, and for this reason privacy and freedom of information must be considered jointly.

3. Recommended Measures to Improve
Personal Data Protection in Ontario

a) To Increase Public Awareness of
Government Information Practices

1) An index should be published of all record collections (whether manual or computerized) held by the Ontario government which contain personally identifiable information. The index should contain: a description of the purpose of each record collection; the content of a typical record; the source of the information; the users; the size of the collection; and what information on the record is mandatory as opposed to voluntary.

2) A report should be published describing typical record collections held by regional governments and municipalities.

3) An annual report should be publicized on developments in record-keeping and computer technology in the Ontario government, describing new systems and the use of data communications, mini-computers, and software packages. The report should also comment on data processing activities in local government.

The above suggestions are aimed at improving public awareness of government record-keeping activities, which is an essential component of data protection. At the same time, they would improve knowledge about the use of records and computers and put to rest some of the more imaginative fears which people have about computer technology. The index would entail an initial start-up expense, but ongoing costs would be minimal, particularly if the index itself was computerized. New developments in computerization often require ministerial or Management Board approval, and submission of such proposals could form the basis for the annual report referred to in recommendation (3).

b) To Facilitate Complaints and
Research into Privacy Issues

4) A data protection board should be established to investigate and resolve complaints into the misuse of personal records; to research

issues of privacy and data protection; and to audit the practices of government agencies and programs at the provincial and municipal levels as they relate to data protection.

The scope of the board's activities in the areas of complaint handling and research need not be restricted to government but could deal also with the private sector. The main purpose of the board would be to identify areas where privacy issues require resolution and recommend detailed solutions to these problems.

A criticism of this suggestion is that the present Commission is already charged with carrying out many of the duties which we would ascribe to a data protection board. However, there are important differences. The data protection board would deal with complaints and carry out research not only on government, but also on the private sector. It would also have terms of reference which were limited solely to privacy issues and would be concerned with freedom of information only as it impinged upon privacy. Our studies on Ontario government agencies left us with the feeling that there was much more to be learned about municipal governments, private agencies and private company practices. In addition, we were impressed by the comments of people involved in implementing privacy legislation in the U.S. — that some form of body which is independent from government is essential to a privacy protection scheme. The New South Wales Privacy Committee has shown that much can be accomplished by a body which specifically undertakes research and

complaint resolution. A number of European countries have adopted the approach of establishing a data protection board either alone or in conjunction with legislated rights of access.

We considered alternative ways of fulfilling the functions of the data protection board. One of these was to have the Ombudsman undertake the responsibility. Another was to make it a responsibility of the Human Rights Commission, as is the case in the federal government. We decided, however, that privacy demands the full-time attention of a separate board, at least at the outset. We would, however, suggest that the data protection board be established for a finite period such as four years, after which reassignment of its functions could be considered. The data protection board should be responsible to the legislature, and should include representation from government, the private sector and the general public.

c) To Promote Government Agency
Awareness of Privacy Issues

5) A "Code of Fair Information Practice" should be adopted immediately by all government agencies in Ontario, as follows:

All organizations maintaining records containing personally identifiable information should be required to:

i) Specify a person to be responsible for each such record collection, whether in manual or automated form, who would ensure that the data was accurate, complete, timely and pertinent in order to assure accuracy and fairness in any determination relating to an individual's qualifications, character, rights, opportunities or benefits made on the basis of such data;

ii) To the greatest extent possible, collect information directly from the subject of the record, who would also be made aware of the uses to which the information will be put and any other sources of information which may be used.

iii) Clearly identify to individuals providing information about themselves what pieces of data were mandatory and why, and what data was discretionary.

iv) Except in situations where revealing the identity of a third party source may result in harm to that person or where a convincing argument can be made that the purpose of the program maintaining the record would be adversely affected, individuals should be allowed full and open access to records which relate to them.

v) Where confidentiality of personal information is not protected in law, determine the purpose for which information is required when access is requested by an individual to whom the record does not relate,

or by an organization not associated with the program for which the record was originally intended.

vi) Record all uses made of personal records by individuals or organizations not associated with the program for which the record was originally intended.

vii) Develop specific policies limiting the release of personal information over the telephone.

Our purpose in proposing that this Code be immediately adopted by all government agencies (municipal as well as provincial) is to encourage them to move towards the practices typically embodied in privacy legislation [see recommendations (8) and (9)]. Use of the Code would be audited by the data protection board.

6) Privacy considerations should be included in the training of all staff involved in handling personal data. This applies particularly to those who collect subjective information, such as social workers, who should be fully aware of the Code of Fair Information Practice.

d) To Assist Individuals in
Protecting Their Privacy

Perhaps the most contentious item in the Code is paragraph (iv) concerning access. This is usually at the heart of most privacy legislation and, of course, freedom of information legislation. Our study indicates that access is not now the norm in Ontario, although there is no reason why individuals should be denied access to most of the government records we examined. The exceptions from access stated in paragraph (iv) are clearly too broad to be more than a guideline, but we would hope that agencies would be encouraged to examine where the real barriers to access lie. To this end we have formulated our seventh suggestion.

7) Where records contain subjective information or information from third parties, or where it is believed that individual access may adversely affect a program's effectiveness, experimental projects should be undertaken to test the demand for subject access and its effect on program operations.

In certain areas of government such as social services, corrections and law enforcement, we came across strong reservations about allowing access to individual records because of information contained in the file. Even with very stringent exemptions from access in some areas it was felt that the demand for access would be overwhelming. During our reviews of the contents of files and in discussions with program staff, it frequently became apparent that these fears might not be

warranted. No doubt, part of the problem is the difficulty of changing a long-standing tradition of secrecy. It may be unrealistic to assume that this change can be achieved overnight. Further, on the basis of our study we are prepared to concede that the relative advantages and disadvantages of individual access in some of these situations cannot be adequately assessed on the basis of theoretical speculation. A series of experiments in selected areas -- opening up files to the subjects of them -- in our opinion would not only reduce the resistance of those who administer files in sensitive areas, but also would facilitate a more confident assessment of the desirability of legislated rights of access in specific and contentious areas. The experiments should be undertaken in cooperation with the data protection board and the results, of course, should be made available to the public.

8) Where confidentiality is governed by statute, there should be strong penalties for breaches of confidentiality. In addition, it should be possible for individuals who are harmed by the release of data which is confidential or which was known to be erroneous, to recover damages in civil action. There should also be provision for costs to be awarded.

Many statutes contain general offence sections providing for summary conviction proceedings and penalties for breaches of confidentiality. Instances of prosecution relating to such breaches have apparently been rare, however. In addition, there is no recourse for a citizen who may

be harmed by such a breach. These limitations significantly reduce the force of confidentiality provisions to the point where they are little more than guidelines. We believe however, that if the confidentiality of information about individuals is of such concern that it needs to be protected by a statutory clause, the protection given should include a strong policy of enforcement and a means of recognizing the harm that could result from breaching confidentiality.

9) We believe that in the long-term, a legislated right of access by individuals to their files is necessary. Views differ as to how quickly such a scheme could be brought into place. We have suggested that an interim period of inquiry and complaint resolution, coupled with the immediate adoption by government agencies of a Code of Fair Information Practices should precede legislated rights of access. An alternative would be to legislate immediately, but to exempt problematic file types entirely from the scheme, in the hope that further investigation by the data protection board would lead to considered and thoughtful amendments to expand the access rights of record subjects of those files. Prime candidates for exclusion, of course, are law enforcement records, and records or portions thereof which contain information concerning other individuals or which were given by a third party on a promise of confidentiality. We are convinced, however, that individual rights of access are fundamental to data protection since it is the individual who has the most to lose from erroneous, incomplete or out-of-date information being used to reach a decision about him/her. In the absence of a

legislated right of access, the pressures inherent in administrative practice which are conducive to secrecy may overwhelm the individual's interest in access. A legislated right of access must, therefore, be an ultimate goal of any data protection scheme.

e) To Establish a Balance Between
Data Protection and Freedom of Information

10) Data protection and freedom of information should ideally be dealt with in a single statutory framework.

Experience in almost all other jurisdictions having separate data protection or privacy acts and freedom of information acts indicates that considerable difficulty may arise from a piecemeal approach. In some American states, consideration is being given to amalgamating the two types of statute in an attempt to remove the confusion both in the agencies affected and among the public in general.

Both privacy acts and freedom of information acts deal with non-disclosure for reasons of privacy, security and the effectiveness of certain government operations, such as law enforcement; both types of statute provide access to records; and both provide an appeal procedure when access is denied. On the other hand, the basic thrusts of the two types of statute are diametrically opposed, and thus inconsistencies develop when non-disclosure, access, appeal procedures and administration are

given separate treatment, and when the relationships between disclosure and privacy are not clearly spelled out.

Finally, we would further suggest that under any freedom of information statute, exemptions from disclosure designed to protect personal records should be strictly defined. Disclosure of personal information to third parties is contrary to the basic principle that individuals should be able to determine for themselves when, how and to what extent information about them is communicated to others. As we have pointed out earlier (in Chapter II), individuals have little control over whether or not their privacy is invaded by government; they are often denied benefits or services if information is not provided. For government, then, to freely disseminate or permit others access to that information for use in unspecified ways is -- we suggest -- a far more serious threat to individual privacy.

PART B: CASE STUDIES

| | | |
|--------------|--|-----|
| CHAPTER VIII | The Social Services | 218 |
| IX | Education | 372 |
| X | Government Personnel Records | 434 |
| XI | Health | 482 |
| XII | Law Enforcement | 530 |
| XIII | Corrections, Probation and Parole | 591 |
| XIV | Personal Property Security Registration | 615 |
| XV | Licensed Driver and Vehicle Ownership Records | 623 |

CHAPTER VIII

THE SOCIAL SERVICES

The purposes of this chapter are to assess the impact of social service record-keeping upon the privacy of social service applicants and clients, to identify problem areas in protecting individual privacy and to evaluate various avenues for minimizing privacy abuse.

To understand fully the implications of social service record-keeping for the privacy of record subjects, we must first examine the relevance of the social services as a topic for privacy investigation. The fact that social service programs intervene in the personal lives of clients has long been recognized, but the rationale for this intervention has only recently been assessed. According to experts in the field, the "peculiar vulnerability of the needy and dependent to official or quasi-official inquiry and surveillance"¹ may arise from several characteristics of modern welfare systems. The first is the inherent conflict between public support of those unable to support themselves (charity) and what is labelled "the public good," or public efficiency. As Handler and Rosenheim note, "the concern for proper limitations on public support is often affected by discernible resentment of

1 Handler and Rosenheim, Privacy in Welfare: Public Assistance and Juvenile Justice, (1966) 31 Law and Contemporary Problems 377.

dependency on the part of those who are tapped to offer the support (i.e., the taxpayers) and by the view that society should tell dependents how to live and behave."² In support of this point, the Canadian Civil Liberties Education Trust Survey noted that:

As long as a recipient hopes to obtain assistance, he cannot expect a secure level of freedom from harrassment. His dependence on public money may make him subject to periodic investigation and interrogation.

3

A second characteristic of the modern welfare system is its "categorical" nature. Need for public assistance⁴ is presumed to be occasional and to result from unusual circumstances.

As such, its disbursement depends on administrative determination of need within broad guidelines set forth by statute, the authorization of payments designed to meet specific individual needs as they arise ... Simply because no legislative determination of social policy can cover all contingencies, the design and administration of public assistance necessarily concentrate on the unique personal circumstances of the recipients.

5

The categorical nature of the social services has been expanded by a growing emphasis on rehabilitation of social service clients.⁶

2 Ibid.

3 Canadian Civil Liberties Education Trust, Welfare Practices and Civil Liberties: A Canadian Survey (Toronto: C.C.L.E.T., 1975) 109.

4 The term "public assistance" does not include aid for the mentally retarded and aged, which are known to be long-term and treated as such in legislation.

5 Handler and Rosenheim, op.cit., 379.

6 Ibid., 393.

Although motivated by the desire to prepare people for independence, thereby ending public support, this approach sanctions intervention into private lives by assuming that social service recipients have problems which cannot be solved by money alone. To discover and treat these problems, society has conferred broad investigatory and decision-making powers upon a variety of professionals such as social workers, psychiatrists, psychologists and administrators.

A third characteristic of the social service system resulting in a propensity to violate individual privacy is the public nature of the interaction between clients and agencies. Merely by entering a social service agency, an applicant leaves his/her private environment, going outside what Muller and Kuhlmann have defined as a situation-specific sphere of privacy, where one can act without fear that information will be disseminated to others.⁷ Social workers who review an application, bank personnel who verify assets, employers who confirm income, postmen who deliver welfare checks, grocers who cash welfare checks and neighbours who recognize the social worker's car will all be witness to the welfare client's status. Especially in small towns, the frequent and public nature of an applicant's or client's interaction with social service agencies will unavoidably endanger his/her privacy.

7 Muller and Kuhlman, Integrated Information Bank Systems, Social Book-keeping, and Privacy, (1972) 24 International Social Science Journal 590.

Finally, perhaps the most important factor affecting individual privacy in the social services is the inability of the poor to defend their rights. Social service applicants are among the least educated, least prepared and least likely to have resources to prevent invasions of their private lives, or to pursue such matters in court. Most applicants approach agencies at times of crisis, when they are even more vulnerable to agency demands for information, especially when refusal to cooperate may mean revocation of needed funds. In this position, some sacrifice of privacy may appear to be a small price to pay in exchange for aid.

Acknowledging that characteristics of the modern social service system have legitimized its inclusion in a study of institutional barriers to individual privacy, we turn to an investigation of personal record-keeping within that system. The case of the Ontario Ministry of Community and Social Services, which administers most public social programs in the province, has been chosen for this investigation. Included in its scope are both provincially directed and provincially contracted, but locally and privately administered, social service agencies.

Approximately 60 people at all levels of responsibility in the Ministry of Community and Social Services and its local agencies were personally interviewed. Four computerized systems in adult services and six computerized systems in children's services were examined, as well as numerous manual and semi-automated systems in both areas. An effort was made to interview field personnel in outlying agencies,

especially social workers and records managers, to gain knowledge of everyday record-keeping practice and its implications for individual privacy.

The following section of the report deals with social service record-keeping for adults. Because the issue of privacy has enveloped different variables in different contexts, problems of privacy in children's services, and the special problems of computerized social service data, are examined in separate sections.

A. Social Services for Adults

1. Volume and Types of Records Held

As of March 31, 1978, the Ministry of Community and Social Services administered sixteen statutes providing services for adults,⁸ all of which require personal records.

8 Ministry of Community and Social Services, 47th Annual Report for the Fiscal Year Ending March 31, 1978 (Toronto, September, 1978) 4. The statutes are: The Blind Persons' Allowance Act, The Developmental Services Act, The Disabled Persons Allowance Act, The Charitable Institutions Act, The District Welfare Administration Boards Act, The Elderly Persons Centres Act, The Family Benefits Act, The General Welfare Assistance Act, The Homemakers and Nurses Services Act, The Homes for the Aged and Rest Homes Act, The Homes for Retarded Persons Act, The Indian Welfare Services Act, The Ministry of Community and Social Services Act, The Soldier's Aid Commission Act, The Vocational Rehabilitation Services Act, The Welfare Units Act.

The nature of services delivered and the process of obtaining assistance varies considerably among the four adult programs investigated, all of which are administered by the Adult Services Division.

Programs for the mentally retarded are administered by the Developmental Resources Branch. The Mental Retardation Facility Services Division provides services to the developmentally handicapped and their families through seventeen government operated (Schedule 1) facilities, ten community board operated (Schedule 2) facilities and four diagnostic and assessment centres. Records are kept from the time the family applies for services, at either a local or government facility or centre. Copies of some types of records and computerized information are retained by the Ministry.

The Family Benefits Act, which provides monthly allowances and other benefits to persons who need long-term financial help, is administered by the Provincial Benefits Branch. Eligible persons include the aged, blind, disabled and permanently unemployable, mothers with dependent children, and those caring for foster children. At present, applications and reports concerning clients are completed in district officers, while decisions concerning eligibility and amount of assistance are made in the Provincial Benefits Branch itself. (Plans exist but have not been implemented to decentralize these decision-making responsibilities.) To determine eligibility and amount of assistance, the Branch assesses the applicant's basic and special needs, family situation, liquid

assets and available income (including medical needs). Records detailing these characteristics are kept by the Provincial Benefits Branch, while evaluations of situational changes are kept by the district offices.

The General Welfare Assistance Act and related statutes (The Homemakers and Nurses Services Act and The District Welfare Boards Act) provide short-term financial aid and special services to those with immediate and emergency needs. Eligible persons may include sole-support mothers, the unemployed, those in ill-health, students, the elderly, and foster parents. In urbanized parts of the province, eligible applicants receive aid from municipalities, which administer the statutes with the assistance and advice of the Ministry Municipal Welfare Consulting Branch. In rural (primarily northern) Ontario, eligible applicants receive aid directly from Ministry district offices or from eighty-five designated Indian Bands. To determine eligibility and amount of assistance, the administering bodies assess applicants' basic and special needs, family situation, liquid assets, available income and living costs. Records detailing these characteristics are kept by the municipalities, Ministry district offices or Indian Bands, depending on the locale of the applicant.

Vocational Rehabilitation Services, also under the Adult Services Division, serves handicapped people with job potential, concentrating on testing, education, physical and psychological adjustment, toward the goal of successful employment. Records are kept from the time of application at a regional Ministry office.

Assuming a broad overlap in programs awarding allowances on the basis of needs, the personal records of at least 203,000 adult clients or about 4% of Ontario's adult population are retained in the Ministry's local or central (or both) holdings, or by municipalities under Ministry auspices.⁹ This estimate does not include "inactive" or "waiting" files, which for the Family Benefits program alone exceed 125,000.

The magnitude of personal records becomes more important when the contents of such records are examined. Table 1 summarizes the nature of information kept in four large records systems of programs administered by the Ministry of Community and Social Services or (in the case of GWA) local municipalities. Four of these contain sensitive information in the following areas:

a) Identification: Individuals listed in both manual and computerized files are identified by full name, file number, birthdate, birthplace, full names of dependents, home address, municipal code, OHIP number and Social Insurance Number, with the exception of the mentally retarded, who are identified in the computerized RSS (Retardation Statistical System) by only three letters of the surname, an abbreviated municipal code and social insurance number.

9 This figure is the sum of estimates given by interviewees. However, the 47th Annual Report for the Fiscal Year Ending March 31, 1978, states that there were 232,850 beneficiaries of allowances under The Family Benefits Act alone in 1978.

TABLE VIII.1

VOLUME AND TYPES OF SOCIAL SERVICES PERSONAL INFORMATION:
SELECTED MANUAL AND COMPUTERIZED SYSTEMS OF PROGRAMS FOR ADULTS*

| Name of Program | FAMILY BENEFITS | GENERAL WELFARE ASSISTANCE | VOCATIONAL REHABILITATION SERVICES | MENTAL RETARDATION FACILITY SERVICES |
|-------------------------------------|--|--|--|---|
| (Name of Computerized System) | Ontario Allowance Program (ONTAP) | Municipal Assistance Information Network (MAIN) | Rehabilitation Information System (RIS) | Retardation Statistical System (RSS) |
| No. of Active Records | 113,500 | 66,500 | 14,000 | 9,000* |
| New Applicants per yr. | 33,000 | 64,000 | 6,500 | 10,000 |
| I.D. INFORMATION | | | | |
| Name | C M | C M | C M | M |
| File No. | C M | C M | C M | C M |
| Unique Code | | | | C M |
| Birthdate | C M | C M | C M | C M |
| Birthplace | M | M | M | M |
| Names of Dependents | C M | C M | C M | M |
| Home Address | C M | C M | M | M |
| Municipal Code | C M | C M | C M | C M |
| OHIP No. | M | M | M | M |
| S.I.N. | C M | C M | C M | C M |
| SOCIAL INFORMATION | | | | |
| Sex | C M | C M | C M | C M |
| Marital Status | C M | C M | M | C M |
| Age | C M | C M | C M | M |
| Education | M | M | C M | M |
| Employment | M | M | | M |
| Family Employment | M | M | | |
| Job Performance | | | M | M |
| Paternity of Children | M | M | M | |
| Social Assessment | M | M | | M |
| Living Arrangement | M | M | | M |
| MEDICAL INFORMATION | | | | |
| Assessment MD | C M | C M | C M | C M |
| Lay Assessment | M | M | C M | |
| Functional Loss | M | M | C M | M |
| Psychological | M | M | M | M |
| Psychiatric | M | M | C M | M |
| FINANCIAL INFORMATION | | | | |
| Income Details | C M | M | C M | C M |
| Assets Details | C M | M | C M | C M |
| Detailed Expenses | C M | M | | |
| Detailed Debts | C M | M | | |
| OTHER INFORMATION | | | | |
| English Fluency | | | C M | |
| Narrative Comments | M | M | C M | M |

* 2,000 of these are children

Key: C Computerized
M Manual
C M Both

b) Social Characteristics: Sex, marital status, age, education, employment details for all contributing household members (including an evaluation of job performance for Vocational Rehabilitation Services), legitimacy and paternity of children, social assessment and living arrangements are commonly recorded in manual systems for both the applicant and spouse. Legitimacy of children and social assessment are usually not computerized.

c) Medical Information: All systems include provisions for some form of diagnosis or medical assessment, which for the mentally retarded and vocational rehabilitation clients includes psychiatric and psychological judgments as part of computer records. (This section on system forms is left blank for those recipients of social assistance whose only criterion for eligibility is financial need.)

d) Financial Information: The Family Benefits and General Welfare Assistance files contain the most detailed financial information for applicants and clients, including all forms of income or revenue, assets, expenses and debts, as well as names of creditors (although names are not computerized). Vocational Rehabilitation records include far less specific financial information, of which only total income and source are computerized. Mental Retardation Facility Services financial records are not part of personal client files, but are kept in manual form by financial offices of institutions for the retarded.

e) Comments: All manual systems include large blank spaces or blank forms for narrative, descriptive comments, which may include remarks meant for internal notice, such as "violent, home visits should be done by male," and remarks intended to assist worker in decision-making, such as "house filthy, not good for Ontario Housing," to remarks meant to reflect subjective judgments, which cannot be included in objective categories, such as "very cooperative, would do well in program." Only the Vocational Rehabilitation Services program computerizes such remarks. Correspondence about the client, reviews of tests performed and other subjective comments are included in all manual files.

2. Record-Keeping Policies and Practices

a) General Protection of Privacy

Individuals interviewed at the management level of adult services were inconsistent in their views of present policy in the area, reflecting the newness of the issue and the diversity of programs within the Ministry of Community and Social Services. The word "privacy" itself held different meanings for different interviewees, most frequently connoting concepts of data security. No overall written policy covers privacy or confidentiality of records, with one possible exception, the oath of secrecy administered by the province to all new employees, felt by one manager to cover the issue adequately. Despite the lack of

written policies, professional ethics of personnel were considered by management to include a high regard for client privacy. However, personnel training emphasizes neither privacy nor confidentiality, and includes no education about client information rights.

Because of lack of policy and discrepant practices at the program, field and agency levels of service, the Ministry has formulated a six-member Confidentiality Committee, charged with developing principles of confidentiality applicable to all programs. The Committee has distilled a list of client-rights oriented privacy principles developed by Legal Services as a result of division reports summarizing present policies and practices, into four abstract principles. These principles are intended to serve as a basis for development of detailed guidelines for each division.¹⁰ Three sub-committees representing the three Ministry divisions have been charged with developing suggested guidelines at the program level, based upon their research of present policies and practices affecting client privacy.

10 Committee on Confidentiality, Ministry of Community and Social Services, Report (Toronto, July 20, 1978). The four principles are: (1) There must be a clearly justifiable and documented purpose for obtaining and storing information, and for releasing information to a person other than the subject of the information; (2) The right of every individual to privacy should be recognized and protected to the greatest extent possible consistent with the public interest; (3) The informed consent in writing of every individual should be a requirement prior to the release of personally identifiable information; and (4) Individuals should usually have access to personally identifiable information about them.

A key issue not yet resolved in the development of social services privacy policy is accountability for records. Directors of some individual agencies contractually funded by the Ministry insist that the agency owns the records and therefore has sole responsibility for privacy and confidentiality of its records, despite the difficulty of establishing legal ownership of information.¹¹ Municipalities also claim record ownership rights over General Welfare Assistance records. The majority of purchase-of-service agreements between the Ministry and service agencies do contain provisions requiring that records be kept and be open to inspection by the province upon request. However, accountability for uniform policies and procedures protecting privacy have not been addressed as yet in such agreements.

The responsibility for third party reports, such as medical or psychological assessments contained in social service record systems, is also open to question. If the third party report writers, who are often not government employees, initiate the records, the agency holding the records may insist it has no authority to reveal their contents to clients or others.

11 See Miller, Arthur, Assault on Privacy (Ann Arbor: University of Michigan Press, 1971) 226, for discussion of personal information as property.

b) Information Collection and Verification

In a brief to the Commission on Freedom of Information and Individual Privacy commenting on types of personal information gathered and recorded on individuals, the Ministry of Community and Social Services notes:

The nature of Ministry programs is such that their administration requires a significant amount of personal information on many clients ... (it) would be unable to deliver its services without such personal and often sensitive information about its clients. 12

Reinforcing this viewpoint, interviewees at the management level agreed that because social services judgments are usually subjective in nature, more information can yield better decisions. No ministry-wide written policy limits the amount or type of information gathered or encourages justification for data elements on records. However, some district managers, supervisors and program directors discourage the gathering of non-factual, subjective and opinionated information, especially from persons other than applicants or clients.¹³

12 Ministry of Community and Social Services, Comments on Freedom of Information and Individual Privacy, brief presented to the Commission on Freedom of Information and Individual Privacy (September 29, 1977) 3.

13 At least one district director has issued a written policy (dated 1977) covering this topic, which states:

Recording should, as much as the program allows, be factual and accurate. Statements which are conjecture and interpretive on the employee's part should not be recorded on case files. Aside from the unfairness of such statements towards the client, it is important to remember that case records may be demanded by an Appeal Board, a Court, or the police.

Inconsistent record-gathering practices in the field reflect the general dearth of ministry-wide policy in this area. Some field workers, counsellors and record clerks consider it necessary to record many aspects of an applicant's or client's lifestyle, habits, emotions and background which might have any bearing, now or in the future, on his/her eligibility, condition or progress in a program. This is especially the case among staff of institutions caring for the mentally retarded or infirm, where the medical model of record-keeping¹⁴ prevails, and for those dealing with Vocational Rehabilitation Services clients, where several attributes, including motivation, are assessed in developing occupational and training plans.

Once per year, Family Benefits workers must re-assess the eligibility and progress of their cases by completing Present Condition Reports, usually while visiting clients' homes. The information collected in these home visits is more likely than information in structured application forms to include subjective narrative, such as comments about emotional or social behaviour, housekeeping skills, possible live-in boyfriends or suspected sources of income. For example, one field worker related her discomfort in working with a file (prepared by another worker) which contained the word VIOLENT in red across the top of a narrative form. Apparently, the original field worker had

14 This model of record-keeping entails the inclusion of a specified number and type of forms in every client/patient folder, a daily logging of activities in residences, and regular contributions to the record by professionals associated with the client/patient.

once mistaken a client's cigarette lighter for a drawn gun and attempted to warn other staff of possible confrontations. Only one field worker among the field workers, counsellors and supervisors interviewed felt prepared to defend his/her subjective statements in a Social Assistance Review Board hearing or other courtroom situation.¹⁵

Written verification policies are also unstandardized. Some managers felt verification should always be presented in support of forms of all criteria in eligibility applications; others thought verification almost unnecessary if audits of forms are regularly completed. The understood policy for the Family Benefits program stated in the Regulations,¹⁶ is that verification is the duty of the intake worker at the individual program level, and must be performed when requested by the Director.

Verification requirements are equally inconsistent among staff at the field level of public assistance programs. Although financial assets

15 The Family Benefits Act, R.S.O. 1970, s. 12(6) states that "the applicant or recipient who is a party to the hearing shall be afforded an opportunity to examine before the hearing any such submission or any written or documentary evidence that the Director proposes will be produced or any report the contents of which the Director proposes will be given in evidence at the hearing." At present, an information summary prepared by the Director or his designee is given in evidence to complaining parties at the SARB. Although this summary may contain subjective statements taken from field notes, it does not identify the field worker responsible for the statements.

16 The Family Benefits Act, R.R.O. 1970, 16, subparas. (2), (3) and (4), as amended to October, 1977.

and income are routinely verified, even this area is open to discretion and interpretation. A Family Benefits worker related a typical case:

Sometimes when I ask for a bankbook, the applicant says that she has no bankbook. I can take her at her word, and usually do, if she seems honest, but if I suspect something, I'll find out where she banks and request a release from her to examine assets, or warn her that her application will be held up until she can produce the book for verification purposes.

Families with children present further verification dilemmas for field workers. Birth certificates of dependent children, notes from schools verifying attendance of children over the age of 16, divorce decrees and support settlements or court proceedings may all be required to verify eligibility. Field workers recognize that each requirement poses a double-edged privacy problem for the client. Obtaining verification documents such as birth certificates from other provinces may be time-consuming but less potentially embarrassing to the client. By requesting the caseworker to obtain verification, the client may speed up the eligibility process but lose control over the dissemination of information about his/her status as a welfare recipient.

In view of the sensitive nature of information gathered from social service applicants and clients, the method of gathering and verifying the information becomes significant. Examples or invasions of physical privacy by social workers in their record-keeping methods have been documented by the Canadian Civil Liberties Education Trust. In a 1971-73 survey of 1000 public assistance recipients in six Canadian cities, most of whom had registered complaints with welfare rights organizations, the Trust found that:

1) In determining whether a woman was "living together with a man as husband and wife" social workers had in some cases checked sleeping arrangements and cupboards, queried landlords, required single women to bring their boyfriends to office interviews, queried clients about their sex lives and asked neighbours to report male visitors.

2) In interviewing unwed mothers, workers had in the majority of cases asked the applicant to name the father, and in some cases questioned recipients on their birth control methods, and/or urged them to give up their children.

3) Workers sometimes arrived unannounced for periodic home visits and conducted inspections of homes without asking permission.

17

Although acceptable information gathering and verification methods are also undefined by written policy, both administrators and field workers who were interviewed believed most of those earlier practices had ceased, with the exception of requesting the name and whereabouts of the putative father of illegitimate children (required by statute). One interviewee believed more positive public attitudes toward assistance recipients and customs in general have greatly influenced social service record-keeping, citing the once-accepted but now prohibited practice of recording inter-racial relationships as an example.

However, field practices differ by region, office and personality. Family benefits field workers interviewed generally attempt to make appointments before home visits, or send postcards to those without phones, although advance notice is not always possible. When writing

field notes, some field workers cover their writing to avoid perusal by clients; no one interviewed had read the contents of field notes aloud or permitted clients to read them during the home visit, although several field workers read completed applications to applicants, carefully explaining all items. The kitchen or living room is the usual setting for interviews, which may take place with friends or relatives present by choice of the client. Office interviews sometimes occur in open reception areas.

Vocational Rehabilitation Services programs and programs for the mentally retarded generally require fewer forms of verification than welfare programs, accepting the client's word for many information items such as birthdate and place. Disabilities must be verified by doctors or hospitals and previously involved agencies. Because these sources have often referred the client to the provincial program, they are already aware of the client's condition and need for services.

Methods for handling information refusal are also unstandardized. When elements such as income are crucial to eligibility decisions, especially in the welfare area, refusal to divulge such information disqualifies the applicant or client from service. However, the policy for handling refusals to reveal less important information is delegated to program personnel.

c) Record Storage

No ministry-wide policy addresses the issue of storage of personal records. All managerial personnel interviewed hoped that program and field staff kept records in closed drawers when not in use, and locked filing cabinets at night, and at least one district director had issued a specific directive covering the topic and knew that staff rigorously adhered to such a policy. Policies for indexing records vary by branch, and program. Although most managers saw no privacy problems in surname, alphabetical indexing and filing, those directing programs for the mentally retarded and disabled use case numbers and coded indexing to insure limited access to client files.

Record storage practices were not standardized among Ministry adult programs examined. Some field workers and counsellors leave completed forms on desks, store them in unlocked filing cabinets in open areas frequented by outside visitors, and regularly take sensitive records home. Others keep only immediate work on desks, store all completed forms in locked filing cabinets within secured rooms, and never take work home. The strictest record security existed in facilities using trained medical record-keepers and in offices where written policy required attention to the subject; the weakest security was observed in certain agencies administering public assistance programs. Indexing followed the same pattern, e.g. the Mental Retardation Statistical System and its manual backup files, which follow a medical model, are indexed by unique case number; Family Benefits case records are

primarily indexed alphabetically, and in one observed case, were separated by the categories, "Deserted mothers," "Singles" and "Others."

The destruction or erasure of records may prevent "labelling" of former social services clients and afford them the opportunity to regain anonymity in society. Yet, policies regarding length of storage time for the records of rejected applicants and inactive clients have received little attention and vary by program and locale. The Developmental Resources Branch, formerly administered by the Ministry of Health, adheres to policies stated primarily in the regulations promulgated under The Mental Hospitals Act and The Public Hospitals Act, which requires records to be kept twenty years, and photographed records to be kept permanently at treatment facilities.¹⁸

In comparison, the policy developed by the Capital and Administrative Services Branch, Records Management Division, states:

18 Department of Health, Memorandum from D.E. Zarfes, M.D., Director of Mental Retardation Services Branch, January 5, 1971, and The Public Hospitals Act, R.R.O. 1970, Reg. 729/78, s. 44, which stipulates that "medical records that have not been photographed in accordance with a practice established by the board pursuant to section 42 shall be retained by the facility for twenty years following date of the last discharge or medical activity rendered at the facility, or for five years following the death of a patient originally treated at the facility, following which period of time they may be destroyed by the Administrator." s. 42 stipulates that medical records photographed for permanent record collections may be destroyed two years after photographing.

Inactive records shall be removed from active ones on an on-going basis (at least annually) by the owning Branch and transferred to the Ontario Government Records Centre or other low cost storage area.

19

Administrators in other programs were unaware of retention policies but often mentioned the time of seven years as appropriate. No rationale for a specific time period was mentioned.

In general, records at central Ministry offices are retained and destroyed according to strict schedules,²⁰ while the often more sensitive field and local agency records are kept according to the personal wishes of the individual worker or counsellor. Some Family Benefits workers, for example, make and keep copies of most forms sent to the Provincial Benefits office; others keep only field notes and client authorization forms. Files of inactive clients are often kept indefinitely by contracted agencies and field offices, sometimes in cardboard boxes or tied bundles in attics or basements. Old records, including tests and diagnoses of illnesses, may be transferred and substituted for new assessments for re-applying clients. One supervisor remembered referring to a client's father's 30-year-old case record for information about the incoming client. Among the programs examined, method of destruction of records varies from supervised burning and shredding to throwing in wastebaskets.

19 Capital and Administrative Services Branch, Records Management Division, Ministry Manual of Administration, February, 1978, s. 200.

20 Ibid.

d) Transfer of Personal Information

The transfer of information from a subject's original records at one location to any other person, office or agency signifies a loss of control over the use and further dissemination of that information. Further, the obtaining of information from any outside party for the original record eliminates subject control over the information-gathering process and creates the possibility of false labelling. In either case, the client's knowledge of and authorization for the transaction can diminish its negative effects and provide the client with a basis upon which to contribute to decisions, contest and correct errors and most importantly, to form a relationship of mutual trust with the agents of social service programs and with governments in general.

Regarding policy in this area, the Family Benefits Handbook states that:

Your field worker or anyone else who works for the Ministry of Community and Social Services will respect the confidential nature of your receiving Family Benefits. 21

However, no overall written transfer policy has been enacted throughout the Ministry, and documents and verbal comments by senior management have expressed a primarily positive viewpoint toward unregulated information exchanges among agencies involved with social services

21 Ministry of Community and Social Services, Your Family Benefits Handbook (Toronto: March 1975) 22.

applicants and clients. A brief to the Commission on Freedom of Information and Individual Privacy, while emphasizing that "the Ministry recognizes the right of individuals to expect confidentiality in their dealings with government,"²² noted seven broadly categorized example groups which might receive individual client information, if necessary:

- 1) other agencies which have a demonstrated "need to know" and which serve the same client
- 2) the Social Assistance Review Board
- 3) the Office of the Ombudsman
- 4) the Police (e.g. for fraud prosecution)
- 5) auditors
- 6) members of the Legislature or Municipal Councillors
- 7) the Courts.²³

The brief did not specify the exhaustiveness of these categories, nor what constitutes a "need to know." Client permission to release information was mentioned only in the first case, not as a requirement but as "often" happening, as was prior source authorization.

Three 1977 memoranda exchanged by senior administrators detailed a "continual exchange of information on clients between District offices and other parties," considerably expanding the categories already

22 Ministry of Community and Social Services, Comments on Freedom of Information and Individual Privacy, op.cit., 4.

23 Ibid. An explanatory letter to the Commission from the Ministry, dated January 5, 1979, stated that "in all but the first category the Ministry has no choice but to release information."

presented to the Commission. One memorandum listed five groups, according to the degree of need to exchange information:

- 1) Other offices of the Ministry, municipal social services, federal social service, private social services
- 2) Schools, banks, insurance companies, hospitals, physicians, etc., where we seek information
- 3) Employers, potential employers of rehabilitation cases, clients' family members, where we seek help or information
- 4) Politicians, lawyers, clients' rights groups, etc. who present themselves as representatives of the clients' interests
- 5) Police, credit companies, landlords, lawyers, merchants, who may seek information from us or we from them.

The same memorandum recommended "that no restrictions be imposed except for sufficient reason," that "it is impractical to obtain specific consents in emergencies or in frequent or trivial instances," and that a "general rule that information may not be released to non-government agencies, or to non-social service agencies" would be detrimental because:

if we cease supplying information to other agencies, they will cease to supply essential information to us ...

24

Differences of opinion prevail at the field level regarding the boundaries of confidentiality. For some, confidentiality is not

24 Internal Memorandum dated December 14, 1977.

Other memoranda were requested by the Director of Social Resources from area executive coordinators, which were summarized in a submission to the Committee on Confidentiality, March 8, 1978.

betrayed by transferring information without client authorization among professionals, because professionals "have high moral standards and protect clients' interests." Others extended the definition to include anyone in government, because government employees all take oaths of secrecy and "carefully weigh the public and client interest when transferring information." No one queried knew whether clients agreed with such broad definitions.

Regarding method of transfer, at the field and local agency level the majority of transfers take place informally by telephone. Incoming telephone requests are usually verified by calling back before information is revealed, as creditors and other private parties have sometimes posed as policemen and agency personnel. When transferrals require written client authorization, forms created for the purpose are not always explained to the client or utilized correctly. One Family Benefits client interviewed complained that she was asked to sign an authorization form before the names of agencies transferring information were entered. As one field worker explained:

Every form requires more time, and the process (of transferral) is so much simpler and more efficient by telephone.

Public assistance field workers, although recruited and hired at the local level, all receive two weeks special training at central Ministry offices. No one queried could remember any specific direction during that training in the transferral of confidential client records, although the fact that client records are confidential is continually

emphasized on the job. To those field workers interviewed, protecting confidentiality refers primarily to the prohibition of discussions of personal client information outside the office and in private settings like coffee shops, or with politicians.

Because of the difficulty in determining what constitutes "appropriate" release, policies regarding employee disclosure of confidential client information have never been uniformly enforced. The most stringent sanction imposed on social workers who had revealed the personal details of their cases to unauthorized outside persons was a written reprimand. No one, within the memories of those interviewed, had ever been dismissed for this type of violation, despite the acknowledged occurrence of hundreds of such cases. Reiterating the dilemma facing managerial personnel in solving this problem, one interviewee stated:

Com Soc employs 12,000 people directly and 10,000 through contracted agencies. With so many different personalities, there are bound to be inappropriate releases of information, but if the release results in helping the client, or identifying a fraudulent application, it is very difficult to punish the employee, especially if the information was given to a politician.

In contrast to social assistance programs, both Divisions serving the mentally retarded follow strict information transfer policies initiated by the Ministry of Health (both programs have recently been transferred from that Ministry) which prohibits release of any information from institution client records to other persons or agencies without the permission of a supervisor and the knowledge and written consent of the

patient or former patient.²⁵ Program employees refuse to answer most telephone requests (except in emergencies) for information about patients or former patients without a letter and accompanying client authorization. Most institutions require logs of all outgoing information transfers, accompanied by patient (or his/her guardian) authorization.

Some administrators of Vocational Rehabilitation Services programs were also less approving of free transfer of personal information without the client's permission, but as yet have required no specific authorizations. (The permission form now utilized contains only a general authorization.) One Vocational Rehabilitation counsellor interviewed had refused to give even basic information about a client without the client's permission to a Family Benefits worker in the same office serving the same client. Vocational Rehabilitation Services administrators have also refused a Ministry of Health request for client lists.

Despite the general managerial attitude favouring free dissemination of information, forms requiring client permission for transfer have increased in recent years. The content and uses of these forms are summarized in Table 2. Noting the fourth column, clearly the majority of these forms have been developed primarily to release verifying

25 M.R. Circular #36/70, The Mental Hospitals Act, R.R.O. 1970, 578/70.

TABLE VIII.2

MINISTRY OF COMMUNITY AND SOCIAL SERVICES: SELECTED PROGRAM SERVICES
FOR ADULTS, SIGNED CLIENT CONSENT FORMS FOR INFORMATION TRANSFER

| Program | Name and Purpose of Client Consent Form | Type of Consent | |
|--|--|---|---|
| | | Program may Obtain Information FROM: | Program may Provide Information TO: |
| Family Benefits and General Welfare Assistance | 1) 80-00-027: Consent for Release of Information (multi-purpose) | Any agency or person listed | Not covered |
| | 2) 80-00-059: Verification of Illness/Disability (for eligibility determination) | Hospital records, ministry file | Medical Advisory Board |
| | 3) 80-00-038: Information for Search of Landing Record (verify age, residence) | Federal Ministry of Employment and Immigration | Not covered |
| | 4) CPP-1006: Canada Pension Plan Authorization to Release Information (verify income) | Federal Ministry of National Health and Welfare | Not covered |
| | 5) 80-00-051: Consent to Obtain Information from Census Records (verify age) | Statistics Canada | Not covered |
| | 6) 80-00-003: Consent to Inspect Assets (verify assets of both applicant and spouse) | Bank or other financial institutions | Not covered |
| Vocational Rehabilitation | 1) 70-00-001: Blanket Consent to relate information about disabled condition and application (Application) | Not covered | "Such agencies, persons or employers as may be concerned with my rehabilitation." |
| | 2) Statement of Release of Medical Records | Medical records of place named | Not covered |
| Mental Retardation Services | 1) 95-00-142: Authorization for Release of Information | Any facility, agency, physician listed | Any facility, agency, physician listed |

information from outside agencies and persons to the Ministry program in question, rather than to recognize any client right to prohibit release of Ministry program-held information to outside agencies and persons (with the exception of the form used by Mental Retardation Services, which specifically lists all transfers in either direction.) When queried about the one-way nature of such forms, managerial personnel replied that the forms were developed only when specific outside institutions and people began refusing to reveal information about their clients to Ministry of Community and Social Services personnel without the client's specific written authorization.²⁶ Ministry administrators pointed to the inconvenience of such forms, saying, in one case:

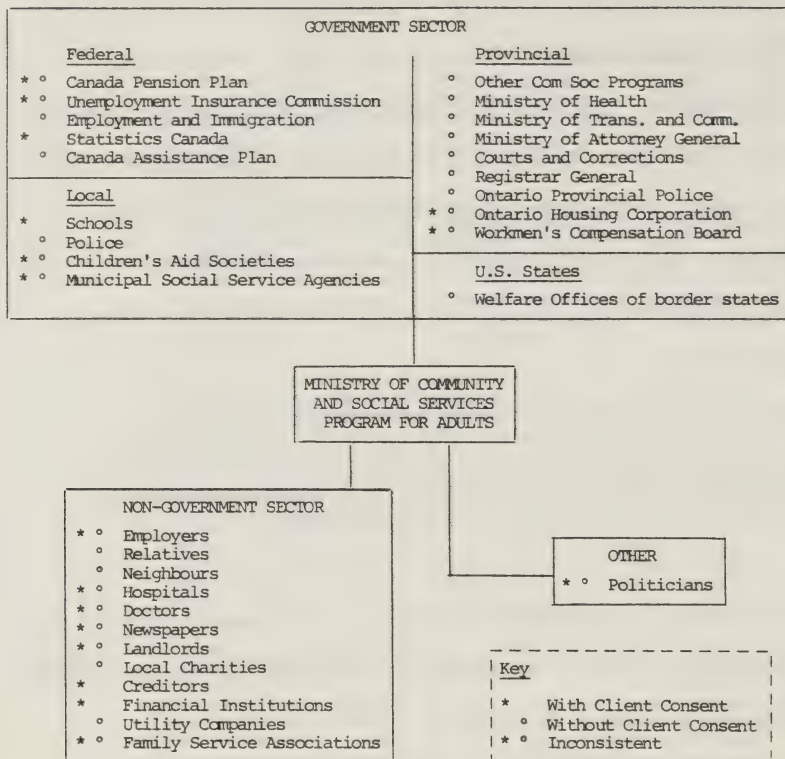
We used to be able to get anything we wanted from anybody. Then, the banks became afraid of being sued if they released confidential information to us, so started asking for client authorization. Now, to see practically anything we have to waste a lot of time getting client signatures.

The types of personal information transferrals which have occurred in practice from and to Ministry of Community and Social Services programs serving adults are detailed in Table 3.

26 This may be related to the fact that some of the first torts of "privacy invasion" accepted by U.S. courts involved unauthorized release of depositors' records by banks to other agencies. An explanatory letter to the Commission from the Ministry, dated January 5, 1979, stated that "examples given for obtaining information are necessary in order to determine eligibility for assistance."

TABLE VIII.3

TYPES OF PERSONAL INFORMATION TRANSFERRALS FROM AND TO
MINISTRY OF COMMUNITY AND SOCIAL SERVICES: SERVICES FOR ADULTS



Although the extent of each type of transfer was impossible to assess in the course of this research project, the volume of personally identifiable information transferrals among private and government parties exceeds that documented in many other areas of government. A substantial number of these transfers take place without the client's knowledge or consent.²⁷ Table 3 is somewhat deceptive in equating all receiving and releasing parties, no matter what the kind or import of information transferred. Examples of kinds of transfers which might pose more danger to a client's eligibility status, participation in decision-making, reputation or integrity are:

In the non-government sector:

1) Reports from neighbours, relatives and acquaintances, which may include rumour, and/or falsehoods about a client's social and sexual behaviour, finances, employment and status of dependent children.

Example: Neighbours may report the licence number of a vehicle seen at certain times near a client's house, intimating a "living together as husband and wife" relationship between the vehicle owner and the client.

2) The release of a client's welfare or disability status to his/her landlord (which was reported in two rural areas) may result in harassment

27 A letter to the Commission from the Ministry, dated January 5, 1979, stated that policy prohibits the release of personal information to anybody without the consent of the client.

or even refusal of a lease by the landlord, who may feel such a status indicates inability to pay rent. In the same vein, the subjective comments of a field worker regarding cleanliness of a house may be utilized by Ontario Housing in deciding whether or not to rent premises to welfare recipients.

3) The transfer of information to and from creditors may affect an assistance or disability allowance recipient's interest rates and credit rating.²⁸

4) The release of confidential medical information regarding diagnosis, prescribed treatment and progress from doctors and hospitals to social service agencies without the client's informed consent may be particularly invasive of privacy to some clients and may be utilized as a device to induce treatment or to evaluate eligibility.

Example: Social workers stationed in some hospitals easily retrieve medical records and verbal reports from personnel associated with their clients. Attendance at clinics or progress in counselling can be utilized by the worker to assess such subjective characteristics as motivation, and sensitive information about past relationships can be used to assess eligibility, without the client's knowledge or consent.

28 An explanatory letter to the Commission from the Ministry, dated January 5, 1979, denied that the Ministry releases any information to landlords or creditors. This denial contradicts the internal memorandum cited on page 179.

In the government sector:

- 1) The police request whereabouts of missing persons and persons accused of crimes from local service agencies. Information revealed without a client's knowledge is often out-of-date, but may result in the questioning of neighbours, acquaintances or new occupants of a given address.
- 2) Workers in facilities for the mentally retarded and other Community and Social Services agencies at one time frequently completed detailed forms about patients from other countries for the federal Department of Manpower and Immigration (now the Ministry of Employment and Immigration). Now the forms are completed only at the specific request of the Ministry, but may include speculative and incorrect data about patients, who are unaware of this transfer which may result in deportation hearings or other severe penalties.
- 3) The Ontario Register General's office freely gives verifying information about births, deaths, marriages and divorces of Family Benefits applicants and their families to the Provincial Benefits Branch central office. Neither Provincial Benefits nor the Registrar-General obtain the written consent of applicants for the release of such records, which may be utilized to revoke eligibility status.
- 4) Computerized eligibility information, case number and Social Insurance Number of Family Benefits, General Welfare Assistance and

Vocational Rehabilitation clients are transferred monthly to the Ministry of Health computer systems so that Drug Benefits Cards may be issued to senior citizens. Such information, although very secure, is linked to client histories containing the nature of all transactions at pharmacies, including type of drug purchased. Unauthorized release of this information could be utilized by employers or insurance agencies to the detriment of record subjects.

5) In May, 1977, a temporary exchange of data was arranged between Michigan and Ontario authorities for the purpose of identifying Family Benefits recipients residing in border municipalities who may have been in receipt of social assistance from both jurisdictions. Without client knowledge or consent, a printout of the entire Ontario roster in these areas was supplied to Michigan authorities for a manual cross-check. Had they known of such an exchange, many clients, especially former residents of another border locality, might have objected to the release of confidential information about themselves to officials in another country.²⁹

6) One form of transfer which directly pits the public's "right to know" against the individual's right to privacy is the relaying of

29 Letter to the Commission, dated March 22, 1979, from Management Board of Cabinet, Management Technology Branch. The letter also stated that although information is shared between border localities on a case-by-case basis, the 1977 roster comparison has not been repeated. No policy has been enacted to prevent such trans-border transfers in the future.

personal social service information to politicians. When locally-elected officials or members of the provincial or federal Parliament request client information, Ministry of Community and Social Services management personnel attempt to provide pertinent records and a reply as soon as possible. Often the client's permission is assumed, especially when the politician states that s/he is acting on behalf of the client. However, such transfers always involve the risks of either political use of information against a client or third party disclosure to the press or public bodies. To prevent the once common practice of publishing welfare recipients' names in local newspapers, The General Welfare Assistance Act specifically states that public disclosure of the names of public assistance recipients is an offence.³⁰ Yet, according to several senior Ministry administrators, local politicians have discussed intimate details of municipal welfare cases in publicly recorded meetings, and have been neither apprehended nor prosecuted under the law for their possibly harmful actions. One interviewee related an anecdote in which a Metro Toronto Council member withdrew a plan to reveal the personal and medical details of a welfare case in an open meeting, but only after a concerned colleague threatened to bring civil action against him in court.

30 The General Welfare Assistance Act, R.R.O. 1970, 383, s. 9, as amended to October, 1977: "No municipality or approved board shall print for public distribution, broadcast or post up in a public place, or cause to be ... made public the identity of any person who is eligible for or receives assistance."

7) Another type of personal information transfer which illustrates the conflict between the public "right to know" and individual privacy occurs when public assistance recipients are suspected of misrepresentation or fraud. The Ministry, municipalities and field offices receive hundreds of calls and letters annually from neighbours, relatives and acquaintances of public assistance recipients (or suspected recipients) accusing public assistance clients of "cheating" in some way, quite often relating information about alleged boyfriends or alleged employment. Ministry policy dictates that such information should at least be acknowledged as one input that concerned citizens have to protect the public purse. However, interviewees at the management level disagreed in their views regarding anonymity and confidentiality of complaint sources, and regarding use of such information in client records. Some managers felt anonymous complaints should be disregarded and not recorded; others felt every complaint should be investigated and logged in client folders. Although confidentiality has usually been guaranteed to third parties, some management personnel held the opinion that a guarantee could no longer be afforded, especially when evidence may be revealed in appeal hearings or other courts. Complaints referred to official fraud investigation units must be recorded on forms specifying name and address of complainant, willingness of complainant to testify in court, and reason if unwilling. When verifying complaint information by contacting employers, other neighbours or other sources, fraud inspectors act without the knowledge or consent of the client. Family Benefits program third party complaints, if leading to suspicion of fraud, are revealed by the Provincial Benefits Branch to the police

(and in Metro Toronto, to a Crown attorney), without the client's knowledge.³¹ Few of these cases are ever prosecuted, but a summary of the record of the complaint and other case information remains on file with the Fraud Review Unit. The actual case records, if viewed or borrowed by the police, are returned to ministry-held files, where they are separated from complaints about record subjects. However, records of the original complaints leading to action sometimes remain in local field office personal case records, possibly inhibiting a client's future application for program eligibility. No ministry-wide policy for all public assistance programs has been issued regarding destruction or elimination from files of unsubstantiated complaints.

e) Research Access to Personal Files

Occasionally, social service organizations receive requests from universities or other institutions to utilize personally identifiable records for research. Although related to other transfer issues, this area is distinctly different in two aspects:

- 1) The end-purpose is usually (but not always) to further the interests of the social service client; and
- 2) The persons performing research are often more restrictively bound to confidentiality by requirements of their institution than even government employees handling files.

31 Until 1970, welfare fraud cases were rarely given to the police or prosecuted in the courts. Now, such a charge is considered like any other criminal charge and is handled accordingly. In a recent 12 month period, over 400 suspected fraud cases were considered by central Ministry officials, of which approximately 90 were given to the police to press charges.

Nevertheless, some research utilizing identifiable records could be just as easily performed with anonymous records, some research may be directly or indirectly harmful to clients interviewed or clients whose records are examined, and the regard of researchers for the privacy of subjects varies by person, training and institution.

In all programs investigated, Ministry policy regarding release of records for research purposes has been strictly formulated to protect the clients' privacy. Research requests are generally forwarded to a program director, who evaluates them on the basis of goals and method. If the research plan is approved, the researcher must sign a user's agreement guaranteeing confidentiality to subjects and/or subject records. If the research involves identifiable records, surveys, or videotaping personal interviews, the written permission of potential subjects is obtained as a condition to participation. A few exceptions have been made to this general policy in the past. For example, a municipal social planning council in Ontario has annually received computer tapes of the personally identifiable records of public assistance recipients in that locale since 1974 without the permission of subjects. In this case, the data was released only after an on-site inspection of the research body's security and after explicit guarantees of anonymity and confidentiality had been signed by researchers.

f) Client Access

The brief by Ministry officials to the Commission promotes no universal policy in the area of client access to records, but instead states that:

The Ministry believes that the sources as well as the nature of information in its files require the Ministry to limit client access on a selective and discretionary basis. 32

The issue of client access was a contentious subject to the majority of management level interviewees, who disapproved of a universal policy allowing clients to see their files. Several reasons for this disapproval were given:

1) Information contained in the file may harm or cause embarrassment to the individual, such as a report that the client is a poor parent or has limited communication skills.

2) Information contained in the file may have been given by third parties who were guaranteed confidentiality. If clients knew their identities, the reputation, physical safety, or relationships with future clients of such parties could be endangered, resulting in a hesitancy to cooperate with social service agencies in the future.

3) Because of the subjective nature of social service record-keeping, clients accessing their files might disagree with many judgments

32 Ministry of Community and Social Services, Comments on Freedom of Information and Individual Privacy, op.cit., 5.

contained within. The brief to the Commission notes that the Ministry could become "engaged in costly litigation to defend such subjective judgments and impressions."³³

4) The client file may include medical information which the client could neither understand nor interpret, such as diagnosis of a fatal disease, or to which the client may have an adverse reaction, such as diagnosis of mental illness.

5) The bureaucratic changes required if clients were allowed to see their files would be too time-consuming and expensive, including the provision of client viewing rooms, the process of reviewing files to remove third party sources, and the creation of double-filing systems, one containing material the client could see and one containing forbidden material.

6) Because most clients have never indicated an interest in reviewing their files, an open file policy would benefit only a few but might arouse suspicion and demands on the part of a previously uninterested population.

In contrast to the majority attitude, some interviewees at the management level saw distinct advantages in allowing and even encouraging full client access to files, including:

- 1) The tendency of social workers to record subjective comments and innuendo unconfirmed by evidence might be stopped and replaced by more accurate, objective, record-keeping practices.
- 2) Clients might become less suspicious and more trusting of public programs and members of the bureaucracy if they felt no information was being hidden from them. One interviewee pointed to psychological research relating sensory deprivation to paranoia, concluding that open files might alleviate some symptoms of the illness among many handicapped social service clients.
- 3) Clinicians might be forced to relay medical terminology in lay terms the client could understand and interpret, assisting clients in dealing with various illnesses and disabilities.
- 4) The paternalistic tendency of many professionals in the social services to overprotect their clients might change, resulting in greater self-respect and personal responsibility among the client population.

Three written policies addressing the access issue were noted to the Commission in statutes and regulations administering adult services.

The Family Benefits Act contains the stipulation that:

The Director may make his submissions at a hearing of the board of review in writing, but the applicant or recipient who is party to the hearing shall be afforded an opportunity to examine before the hearing any such submission or any

written or documentary evidence that the Director proposes will be produced or any report the contents of which the Director proposes will be given in evidence at the hearing. 34

According to this section, Family Benefits clients who appeal decisions might be afforded more knowledge of the contents of their files than those who do not appeal decisions. In practice, however, the Director rarely provides detailed file information to the client before the Social Assistance Review Board, but instead provides an administrative summary which does not identify information sources. Some senior administrators interviewed felt that more detailed file information identifying sources should be given to the appealing client, to assist him/her in stating a case and to promote accountability among record-collectors.

Programs for the mentally retarded or infirm can permit client access under the discretionary policy stated in The Mental Hospitals Act regulations if the client is in an institution governed by that statute:

No disclosure shall be made from the records of a patient without the authority of the officer-in-charge ... (who) may disclose or authorize the disclosure of information from the records of a patient ... where it is clearly not against the best interests of the patient.

35

34 The Family Benefits Act, R.S.O. 1970, c. 157, s. 12(6) as amended by S.O. 1971, c. 50.

35 The Mental Hospitals Act, R.R.O. 1970, 578, s. 3(4).

However, administrators of these programs stated that this regulation and one governing The Public Hospitals Act³⁶ are utilized primarily to deny access to requesting individuals.

One often-mentioned management rationale for the lack of policy favouring open files was the relative novelty of the subject. Very few requests to examine files have been received by provincial administrators, and no cases taken to the Social Assistance Review Board have specifically been appealed on the basis of denial of access to records.

Contrary to the assertions of managerial personnel, numerous requests for client access to personal files were reported by program and field level personnel. Some of those working at the field level, especially medical records personnel at institutions, react to such requests with firm negative answers, relying on "unwritten" policy governing the issue.

Others working at the field level have generally not opened files to requesting clients, but expressed confusion in handling such requests, as a result of the lack of written policy on this point. Most have

36 The Public Hospitals Act, R.R.O. 1970, 729, s. 48(5), as amended to O. Reg. 986/78 states "A board may permit ... a person who presents a written request signed by, (i) the patient, (ii) where the record is of a former patient, deceased, his personal representative; or (iii) the parent or guardian of an unmarried patient under eighteen years of age ... to inspect and receive information from a medical record and to be given copies therefrom."

deferred requests to supervisory staff who have verbally summarized records if the client has been insistent. However, a few ^{of} interesting exceptions to the rule have occurred. One former Vocational Rehabilitation counsellor had agreed to put only those forms in one client's file that the particular client had seen and approved himself. The client feared that biased documents incorrectly presenting his case might be entered in his file, and was reassured, through this method, that in fact no errors occurred. To make sure that assumed confidentiality of third parties was not violated, the counsellor contacted all clinicians and other agencies assessing the client and obtained their cooperation in showing test results to the client before sending the results to the counsellor.

Many of those interviewed at the field level objected to open access for the same reasons as managerial personnel, and emphasized the fear that the assumed confidentiality of third parties would be broken by such a practice, resulting in a decrease in third party cooperation. However, field workers reviewing files during interviews often concluded that clients were fully aware of the sources and nature of information about them anyway, so would be unlikely to adversely react to access opportunities. In further support of client access, third party confidentiality was deemed a poor practice by many interviewees, who felt it promoted a lack of accountability for important judgments about people in often desperate need.

From a practical viewpoint, complete Family Benefits files can be accessed only with great difficulty at the present time, especially by clients living outside Toronto. Most standard and all medical records are permanently filed at the Provincial Benefits Branch, while field notes, letters of referral and other important documents contributing to eligibility decisions are usually retained at field offices. However, the Capital and Administrative Services Branch, Records Management Division, does provide an avenue of central records access which now may be utilized only by administrators but which could be easily adapted for utilization by clients:

The Records Centre will ensure half day delivery service of records requested within the Toronto area or if requested, provide verbal information from the records (and) a reference room for personal on-site consultation to the records. 37

The client records of other programs are primarily filed and catalogued in one records area at a field location, where access could easily be attained under private and supervised conditions.

B. Social Services for Children

Social service record-keeping for children envelops many of the same privacy issues as record-keeping for adults. Policies and methods governing information gathering, verification, storage and retention,

37 Capital and Administrative Services Branch, Records Management Division, op.cit., section 205.

limitations on record transfers, outside research requests and accessibility of personal files to record subjects all affect the privacy of both child and adult social service clients. The problems of ownership of files, especially where contracted agencies keep important records, statutory requirements to "protect the public good," which involve investigations of sensitive personal histories, and computerized data protection have further complicated privacy issues in both child and adult social services.

In addition to problems common to both spheres, privacy protection for children involves questions unique to that sector of society not yet legally considered adults:

1) Age of maturity: Children, by virtue of their minority status, have as a general rule been regarded both by custom and by the law as incompetent to sign contracts, give consents, bear witness, vote, and generally participate in decision-making processes. However, the question of maturity, or ability to handle the effects of decisions, has usually been a mitigating factor in particular cases involving privacy of children, such as those involving permission for teenagers to purchase birth control devices without parental knowledge. The societally determined age of maturity is a crucial component in resolving this question. This society does not consider the onset of puberty, an indication of physical maturity, as important as indicators of mental maturity, such as rationality, composure, verbal fluency, self-confidence, and emotional stability. The former usually occurs between the ages

of 11 and 15; the latter develops gradually from the approximate ages of 5 to 18.

The variability of maturity has serious implications for personal record-keeping in the social services, resulting in the following problems:

- . At what age should a child, rather than his adult guardian, be the source of record information?
- . At what age should a child be allowed to keep personal information away from the purview of adult guardians?
- . At what age should a child, rather than an adult guardian, be allowed to refuse consent for record transfers which might affect treatment by other agencies?
- . At what age should a child, rather than adult guardians or a sponsoring program or agency, determine which third parties, such as doctors, may evaluate and contribute that evaluation to the record file?
- . At what age should a child be allowed to see the contents of record files held by social agencies?

At present, these problems are handled on a highly personalistic basis in Ontario, although certain policies universally deny all children under the age of 18 any rights in record-keeping. In grappling with the competency issue, the New South Wales Privacy Committee has suggested that children be divided into three age categories. Children under 14 are generally regarded as too immature to handle responsibilities and rights of record-keeping, which should be delegated to adult guardians. A more individualized approach is suggested for those between 14 and 18, who are considered "in the transition period to adulthood." Those over 18 are considered mature and capable enough to

exercise their rights and responsibilities, and therefore old enough to exclude adult guardians from the record-keeping process.³⁸ Such an arbitrary age division may or may not apply to Canadian youth. The Children's Services Proposed Standards and Guidelines for Children's Residential Care Facilities suggests that Ontario youth be actively involved in institutional decision-making about themselves from the age of 12 onward, and have exclusive rights of access and control over treatment decisions at 16, considered the "age of emancipation" in this province.³⁹

2) The onus upon society to protect children: In the same manner that protection of the public good often conflicts with protection of the private good in adult social services, the protection of children may conflict with the right of privacy for children and their families. Since the inception of Children's Aid Societies in the 1890's, Canadian institutions have increasingly sanctioned a public advocacy role to defend children against cruelty, neglect, misuse and manipulation by their families. This role has involved a greater emphasis on a child's right to a happy, healthy existence, especially in medical decisions. One example is the growing intolerance of the courts, especially in the United States, for parental refusals to consent to religiously prohibited

38 New South Wales Privacy Committee, Guidelines for the Operation of Personal Data Systems (exposure draft, Sydney, Australia: April, 1977) 17.

39 Children's Services Division, Children's Residential Care Facilities: Proposed Standards and Guidelines (Toronto, September, 1978) 40-41.

medical treatments, such as blood transfusions, for their children. The courts have overridden the requests of parents in these cases, rationalizing that parents could not cause the death of their children and had no right to invoke the child's right of privacy or even the child's religious beliefs as the reason for withholding treatment. The child's legitimate right to privacy has been interpreted by the courts as the right to live a normal life, unencumbered by harmful family customs.⁴⁰

The more active protecting role of society for children has required record-keeping which can invade the privacy of the home and the family. Supporting this contention, the Children's Services Division of the Ministry of Community and Social Services recently outlined its responsibilities which require data collection, including:

Monitoring and Serving High Risk Population

Certain families in the community have the potential for having children with a higher risk of developing special needs. These include children who have physical or cognitive abnormalities or who are socially disadvantaged. By identifying this high risk population, families with children having these characteristics could be monitored and provided with appropriate prevention services.

41

40 Brant, Jonathan, "The Child's Right to Privacy", Harvard Educational Review (1974) 42. In a similar Canadian case, Pentland v. Pentland (1977), 5 R.F.L. (2d) 65, the court revoked child custody rights from a divorced mother who refused blood transfusions for her seriously injured teenaged son, and granted custody of the boy to a relative who agreed to proper medical treatment.

41 Children's Services Division, Consultation Paper: Information Systems Development for Children's Services in Ontario (Toronto: May, 1978) 7. In a letter from the Ministry, dated January 5, 1979, the Commission was assured that the intent of Children's Services' data systems is not to collect large amounts of personally identifiable data, but to identify high-risk populations. However, large amounts of personally identifiable data are already collected (cont'd)

Child abuse registries, detailed social histories of prospective foster and adoptive parents, documentation of physical punishments by school personnel, and public health records of communicable diseases and innoculations all exemplify the massive data collections about families which have evolved from the societal decision to protect children. The alternative, trusting the private familial sphere and the small community to discover and deal with child abusers -- to ensure the raising of happy, healthy, uninjured children and to prevent the spread of disease -- has become unfeasible as the population has become more mobile, urbanized, and less family-centred. Until these trends are reversed, the public domain will probably continue to gather and keep more personal, private records about children and their families.

3) The family casebook: A related problem which further complicates the children's privacy issue is the practice of organizing records around the family, rather than the client. In the past five years, social agency personnel have accepted the premise that a child is a product of familial environment, and that personal change can occur only with changes in that environment. As treatment has involved more and more members of a child's family and friends, case records have expanded to include regularly-gathered personally-sensitive information about more and more persons related to that child. The implications of this record-keeping trend for the privacy of all those included in a record file are many. Social agencies must confront such difficult questions as:

41 (cont'd) by Children's Services. Additionally, it is difficult to comprehend how "families can be monitored and provided with appropriate prevention services" without any identification of families and children served.

- . If a child is encouraged to read his/her file, should his/her mother's remarks about the negative impact of Uncle X upon his/her sexual development be removed, especially if Uncle X has no knowledge of the remarks and still influences the child's life?
- . If the child's casebook includes the results of many interviews with an uncle, should the uncle be allowed to review any or all of the child's file?
- . Should family records be carefully separated before transferral to another agency which will treat only one member of the family?
- . Should all those mentioned in a family casebook be given the opportunity to refute allegations contained in the record?

To address privacy issues completely, social agencies must ask whether the very existence of family casebooks seriously endangers individual privacy of children. However, an affirmative answer by no means assures the end of the family approach to social work, which has been documented by many to be successful in helping child clients solve problems and lead happier, more productive lives.

4) The new start: Although modern society often indelibly bestows labels such as "criminal," "bad apple," "lazy," "welfare cheater," and "poor mother" on adults, it hesitates to place children in such rigid categories. Children, considered more capable of change than adults, are more easily forgiven their misdeeds, (which are often viewed as childish mistakes) and given many "second chances" to start again on a path of normality. Reinforcing this attitude, social reformers have established juvenile court systems that avoid adult penalties and prohibit the release of names to the media of children in trouble. They

have also designed alternative schools where children once thought disruptive may try anew in a more lenient environment, and have encouraged social agencies to allow children to change counsellors until a relationship satisfactory to the child is found.

If record-keeping practices are to conform to the societal direction giving children a new start, provisions must be made to: destroy records after treatment and at a certain age; prohibit the transfer from one agency to another of records that negatively label a child; keep generalized judgments about a child out of his/her record; update carefully and regulatly data such as test scores contained in a child's record; and, encourage child subjects to review and correct errors in their records. Such practices may conflict with the high value society places on the protection of children. An example of such a case involved an Ontario teenager, where the existence and transfer of a record labelling the child as suicidal might have saved her life.⁴² The difficult task of balancing the protection of a child's well-being with the privacy of the child or the child's family confronts all social service agents who keep records about children.

The problems these issues pose for social service record-keeping about children have been explored through an investigation of nine records systems held by the Children's Services Division of the Ministry of

42 "Jury told girl, 14, did not belong in school where she died," Globe and Mail, November 26, 1976.

Community and Social Services and its contracted agencies, supplemented by interviews of 31 personnel with knowledge of these systems.

The Children's Services Division administers several statutes providing a large variety of social services for Ontario juveniles.⁴³ Due to the recent transfer of mental health, corrections and court programs from other ministries, the Division now is responsible for what has been termed one of the most comprehensive children's social services packages in North America. By program surveyed, these services include:

- 1) Children's Mental Health Services, providing both residential and community care to emotionally disturbed children and those with other psychological problems. Thistletown Centre is included in this Branch;
- 2) Community Liaison and Child Welfare, providing support services to Children's Aid Societies and "integrating a wide range of services to children and their families including alternate guardianship, foster and residential care, family counselling ... and adoption."⁴⁴ The

43 According to the Ministry's 47th Annual Report for the Fiscal Year Ending March 31, 1978, these statutes include: The Child Welfare Act, The Child Welfare Municipal Payments Continuance Act, The Children's Boarding Homes Act, The Children's Institutions Act, The Children's Mental Health Centres Act, The Children's Mental Hospitals Act, The Children's Services Transfer Act, and The Day Nurseries Act. Due to reorganization, the list has been expanded to include The Provincial Courts Act, The Training Schools Act and The Unified Family Court Act, as referenced in Children's Services Legislation Summary (Toronto: June, 1978).

44 Ibid., 16.

Child Welfare Branch also administers day-care programs throughout the province;

3) Juvenile Corrections, providing probation, after-care and support services for juveniles who come into contact with Family Courts.

1. Volume and Types of Records Held

Officials at the senior management level of the Children's Services Division estimated that active case files on approximately 112,000 children in Ontario are held by the Division or its agents, but that the total number of active, inactive and pending children's files may exceed 200,000. A considerable amount of overlap exists among all the children's services filing systems, as children may be channelled through a number of agencies and reappear frequently for various services. The volume and contents of systems examined are summarized in Table 4. The table reveals that both official approximations and the TEIGA-produced annual Catalogue of Statistical Files greatly underestimate the number of personal records on children and their families held by the Ministry of Community and Social Services and its contracted agencies in Ontario. Assuming overlap among many of the record systems in Table 4, the existence of at least 287,000 children's files has been documented by our research. This number excludes the case files of fifty Children's Aid Societies outside Toronto, several municipalities other than Toronto which receive funds for day nurseries, the manual

TABLE VIII.4

VOLUMES AND TYPES OF INFORMATION COLLECTED BY
SELECTED RECORDS SYSTEMS OF CHILDREN'S SOCIAL SERVICE AGENCIES**

| PROGRAM & NAME OF SYSTEM | CHILDREN'S MENTAL HEALTH STATISTICAL INFORMATION SYSTEM (CMHSIS) | THISTLETON REGIONAL CENTRE | CHILD ABUSE REGISTRY | TORONTO DAY NURSURIES INFORMATION SYSTEM |
|--------------------------------|--|--|--|---|
| No. of Records | 10,000 | 4,800 (since 1957) | 9,000 | 12,000 |
| System Type | computerized, centrally-held | manual, agency-held | manual, centrally-held | computerized, municipally-held |
| Identifying Data | code consisting of part of name and birthdate, unique case no. | name, address, municipal code, (blank for) SIN** OHIP no., case no., birthdate | name, address, case no., child's birthdate, aliases and any other known ID of alleged offender | name, address, municipal code, SIN, OHIP no., home/bus. phone, birthdate, date arrived in Canada |
| Social Data | previous placement type, sex | situation in community, sex, social history, sibling info | relationship of offender to child, nature of abuse | immigration status, sex, complete social history, sibling info |
| Education Data | none | school type & name, full school report | school report if relevant | previous nursery schools attended |
| Medical Data | no. of previous treatments, present problem | present diagnosis, complete clinical record, psychological treatment of other family members | doctor's report, hospital report | physical exam of child, psychological data if relevant |
| Court Data | wardship status | wardship status, court records if relevant | all relevant court action | none |
| Financial Data | none | kept separately | none | income, assets, budgetary items, family allowance, welfare data, form 7 |
| Case Management | referral source, place previously treated, changes, disposition, termination | progress, goals, problem list, termination | CAS action, court action | kept at nursery |
| Other | none | all documentation (letters, worker narratives) | narrative | "as much information as possible about family and child" |

** As yet, the blank for SIN provided by Ministry of Health forms
has not been filled.

TABLE VIII.4 (Cont'd ... 2)

| PROGRAM & NAME OF SYSTEM | PROVINCIAL WARDS RECORDS | JUVENILE INFORMATION SYSTEM (JIS) | JUVENILE PROBATION SYSTEM (JPS) |
|--------------------------------|---|---|--|
| No. of Records | 13,000 | 2,000 | 8,000 |
| System Type | manual, centrally-held | computerized, centrally-held | computerized, centrally-held |
| Identifying Data | name, address, municipal code, birthdate | name, address, municipal code, height, weight, hair colour, build, OHIP no., ward file no., birth date/place, scars, disabilities, aliases | name, address, municipal code, case no., birthdate, aliases |
| Social Data | initial report on family and social situation | living situation, religion, Indian status, language used, sex, cultural identity | type of accomodation, religion, Indian status, sex, present family constellation, clubs, hobbies |
| Education Data | full report from school | school address, phone no. | school name/address/ phone no. |
| Medical Data | psychological testing, medical reports if relevant | disabilities, special medical conditions | none |
| Court Data | all court reports, wardship status | court location, previous probation & court appearances, wardship status | judge, court, county, details of probation order, wardship status |
| Financial Data | all relevant, including welfare info | family allowance no. | none |
| Case Management | all actions on case | movements and activities, referral source | previous placements (when/where) |
| Other | all documentation (letters, pre-sentence report) | narrative section (comments) | narrative section (comments) |

TABLE VIII.4 (Cont'd ... 3)

| PROGRAM & NAME OF SYSTEM | MINISTRY CHILD WELFARE RECORDS | METROPOLITAN TORONTO CHILDREN'S AID SOCIETY | | | |
|--------------------------------|--|--|---|---|--|
| | | 1) PHOTO FICHE | 2) CHILD SERVICES INFO. SYSTEM | 3) RESOURCE INFO. SYSTEM | 4) FAMILY SERVICES INFO. SYSTEM |
| No. of Records | all records since 1890* | 250,000 | 20,270 ⁺ | 2,041 ⁺ | 42,144 ⁺ |
| System Type | manual, centrally-held | manual, agency-held | computerized, agency-held | computerized, agency-held | computerized, agency-held |
| Identifying Data | name, address, municipal code, other info depends on local CAS | name, address, case no. | name, address, parents SIN, case no., home/bus. phone, birth date/place, aliases, appearance | name, address, municipal code, home phone | name, address, municipal code, SIN, OHIP no., case no., home/bus. phone, birth date/place, aliases, marriage date/place |
| Social Data | all background info for adoptees, social data for others, depends on local CAS | nature of parents relationship & employment, ethnic origin, sibling info, complete social history | type of accom., religion, sex, cultural ID, parents marital status, mother's prior relationships, sibling info | details about children in care | type of accom., religion, sex, cultural ID, marital status, sibling info, evaluation on 16 social factors |
| Education Data | school reports | school reports | school name/ address/phone, grade | none | parents education status, child's school |
| Medical Data | health assessment, adoptee medical history, other details | physical & psychological assessments | reason for referral, hospital code | perceived health care of children | reason for service, hospital, doctor's name/address/ phone, judgment of "intel-emot" & "health" factors, "pregnancy" |
| Court Data | all documentation, court reports | all documentation, court reports | legal status, reason for service | none | legal status, reason for service |
| Financial Data | complete documentation of status | complete documentation of status | financial rates, subsidy status | none | income source, ownership/rental/ OHC of home |
| Case Management | all actions on case | all actions on case | all actions on case | date of last evaluation | referral source, progress, changes, termination |
| Other | all documentation (letters, worker narratives) | all documentation (letters, worker narratives) | admission details, family whereabouts | complete evaluation on 27 criteria | evaluation on 42 factors (material, management, social, health, intel-emot, child abuse) |

* The actual number of records is not known.

+ All of these records are duplicated in the photo-fiche system.

records of over 700 youth residences and seven observation and detention homes throughout the province, and at least two filing systems so large or cumbersome (including the centrally held Child Welfare records) that systems managers could not estimate the total number of records contained within. Additionally, plans have been proposed for two new record systems, a Prevention Management System which might identify high risk populations, and a Case History Locator Project.⁴⁵

Types of data gathered, with examples, include:

1) Identification Data: Name, address, case number and birthdate are most commonly utilized, although phone number, Social Insurance Number and OHIP number of parents are often gathered. Systems based on the correctional mode record such identifying characteristics as aliases, scars, disabilities, eye colour, hair colour, weight and build. No consistency has been attained in indexing mode among the several systems, some of which utilize full name, others of which utilize elaborate unique codes common to several systems.

2) Social History: Type of accommodation (e.g. rented or owned, single-family or multiple-dwelling), present living circumstances, religion, cultural identity (Indian status, language), sex, education

45 Children's Services Division, Consultation Paper: Information Systems Development for Children's Services in Ontario, op.cit., 47-48. If the Prevention Management System is implemented as presently envisioned, it could replace a number of existing systems with one which does not personally identify clients.

(including name of school, name and phone number of contact, and school reports for most systems), detailed information about siblings, and a narrative social history are included in most files. Some systems also record country of parental origin and parental immigration status; one records details of parents' previous relationships. Nature of employment may also be recorded for parents. The cultural identity or ethnic origin variable, like so many quantified social variables, exemplifies the problem of exhausting a large number of possible categories with a discreet, small number of codes. One system allows nine such codes; another allows 52.

3) Financial Information: The most detailed financial information is gathered from parents of day-care attendees, who must prove need by cataloguing all contributions to income and all monthly expenses to qualify for subsidies. Some systems document various amount of financial data, such as basic financial information of parents, while one system computerizes the Family Benefits allowance file number.

4) Medical Information: Most systems include patient or client category, a lay assessment of problem (i.e. disabled: yes/no), types and places of previous treatment, psychological and psychiatric testing results, medical diagnoses, and details of physical examinations. One system gathers information about the psychiatric treatment of other family members. A complete clinical record with progress reports is part of the manual personal files at institutions for the mentally retarded, emotionally disturbed and mentally ill. The Child Abuse

Registry contains doctor-recorded descriptions of injuries and scars received by abused children.

5) Court Information: Because of the amalgamation of children's services among several ministries and the court-origin of many referrals, most children's services systems include court information such as name of judge, place of court appearance, disposition, conditions of the child's probation, institutionalization, and wardship status. Some include records of previous court appearances and dispositions. The Child Abuse Registry contains information about any court action taken against alleged adult child-abusers.

6) Agency Action: Included in most record systems are data such as date of admission into program, dates of assessments, identification of the services requested by the referral source and the client's family, goals and objectives for the child and the child's family, the progress made toward goals, and status of the case at termination of service. The most elaborate system examined, the Metro Toronto Family Services Case Management Information System, computerizes a great number of subjective case management variables, such as improvement in "child management skills," "ability to handle social adjustments," "relationship factors," "dependency vs. self-sufficiency" and "sexual adjustment of child."

7) Narrative Comments: All computerized and manual systems, with the exception of the Children's Mental Health Statistical System, include spaces on forms for narrative comments and opinions.

When compared to adult services files, two striking characteristics of the children's services information systems emerge: their inclusion of a greater amount of data about significant relatives, such as parents and siblings; and, their inclusion of a greater number of social history variables which cover almost every aspect of a client's past life and present circumstances.

A third characteristic peculiar to children's services information systems is the overlap of data from all types of social services, including education, health, social assistance and justice, within the same client record. In general, no clear boundaries can be distinguished among the many contributors to a child's or family's assessment and progress, even if they originate from several ministries, because all variables in a child's environment are considered related and relevant.

A recently issued document by the Children's Services Consultation Task Force indicates that the trend toward gathering larger and larger amounts of vaguely defined data elements from many sources about not only clients, but also prospective clients, may be increasing.

Rationalizing that

it will be important for each community to know of families with high risk children in its area so that these families can be monitored and given service, as necessary, to reduce the probability of their children developing special needs,

the document outlines the probably necessity of collecting data from schools, public health services, social agencies, law enforcement agencies and hospitals. Hospitals, for example, would contribute the

following data to identify such children at birth: certain medical complications; prematurity (less than 3 lbs); physical handicaps; mother less than 18 years old; and more than six children in low-income family.⁴⁶

2. Record-keeping Policies and Practices

a) General Protection of Privacy

The impact of massive existing and planned data collections on the privacy of children and families in Ontario has been explored by at least three Children's Services Division documents.⁴⁷ However, no written policies covering privacy and confidentiality of clients and their records have been issued by the Division's management. No standards and guidelines regulating data collection, verification of sensitive or critical information, maintenance and security of personal records, transfer and sharing of information, and personal access to subject records have been set for the Division as a whole. Only Juvenile Corrections programs, transferred to the Ministry of Community

46 Ibid., 19.

47 See, for example, the aforementioned Consultation Paper on Information Systems Development, the Consultation Paper on Legislative Amendments and the Report of the Task Force on Information Disclosure (October, 1979).

and Social Services, and scattered field agencies and institutions have formulated policies in the area; but these are inconsistent and contradictory among jurisdictions.

Despite the lack of clear written policy, interviewees at the management level appear to be aware of the seriousness of privacy and confidentiality issues and of the need for policy development throughout the Division. One interviewee expressed amazement "that we have reached this level of service without ever seriously broaching the topic." An impetus for careful attention to the issues by both management and field personnel has been recent public exposure of problems in the area. For example, publicized child abuse cases, which involved the lack of information exchange by social agencies,⁴⁸ and lobbying efforts of adoptees to pass legislation allowing disclosure of their biological parent identities,⁴⁹ have provoked investigations into the feasibility of formal information transfer arrangements and of client access to personal records held by the Division.

Children's Services management has begun the policy-making process in these areas by striking a Case Information Disclosure Task Force charged with examining issues and problems in the area and formulating

48 For example, "Watchdog for Minor's Children?", Globe and Mail, December 1, 1977.

49 Ministry of Community and Social Services, Committee on Record Disclosure to Adoptees, Report (Toronto: June, 1976) 2-6.

alternative solutions. The Task Force meets monthly and consists of representatives from the provincial administrative office (including legal and records management staff), public agencies, private institutions, the medical field, the educational field, and adult social services. By August 1978, this committee had gathered bibliographical materials, circulated reports of related task forces, identified areas to be addressed,⁵⁰ and developed three draft working papers for consideration by the Division. One paper clarified the purposes of case record systems, another outlined proposed client rights, and a third paper proposed guidelines and standards for personal data record systems, based on a project of the New South Wales Privacy Committee in Australia.⁵¹

In addition to the comprehensive work of the Task Force, Children's Services Division personnel have investigated the legal implications of subject access to personal records, and have contributed a memorandum to the Ministry Senior Management Committee detailing types of confidential information held by children's programs and problems

50 These included: (a) definitions of key concept, including "case record" and "consent;" (b) recognition of philosophical approach of children's services, one centered on the welfare of the child; (c) recognition of important issues, such as transfer, retention, ownership, source and release of records; (d) evaluation of problems experienced in the U.S. between "freedom of information" and "privacy" interests; (e) comparison of provisions in provincial statutes governing the issues; and (f) consideration of problems involved with implementing policies, such as worker protection, retroactivity, clinician anxiety, and arbitration of complex cases.

51 The final report of the Case Information Disclosure Task Force was released to the field as a consultation paper in October, 1979.

related to data security. They have also formulated privacy standards for information systems and residential services, utilizing agency and public input gathered through consultation papers on these subjects.

b) Information Collection and Verification

Stated justifications for collection of the various data elements in Children's Services record systems are primarily unwritten administrative guidelines and past practice, and have followed the social services trend of discovering and recording as much as possible about the client, his/her circumstances, relatives and other environmental influences. Few statutes or regulations specify information to be gathered to satisfy regulatory requirements, although a few (e.g. The Mental Health Act) allow institutions to gather whatever information is necessary to implement the statute. In general, administrators have not systematically questioned the necessity of including subjective information (e.g. "appearance"), information from a variety of sources other than the client (e.g. teachers), data elements not directly related to the provision of services (e.g. "family allowance file number"), or very sensitive elements which might endanger the privacy of the client (e.g. "previous relationships of parents"). The nature and minimum amount of information necessary for provision of services has not been determined for any system examined.

Despite the lack of official policy limiting data collection, interviewees at the management level have begun to question the perceived necessity of gathering so much personally sensitive data, and to recognize that not all data collected are required for decision-making purposes. Division management also have recognized the confidentiality and security responsibilities imposed upon them by the very existence of personal data in files. With these concerns in mind, the Case Information Disclosure Task Force is attempting to clarify the purposes and information needs of a case record system. A draft working paper on the subject includes the statement that

Records that assist case workers in their assessment and treatment, must clearly articulate the relevant history, the present strengths and weaknesses of the child and family, and the formulation of the case with appropriate plans and goals. 52

Although terms such as "relevant history," "present strengths and weaknesses" and "appropriate plans and goals" are not specific in describing data elements, the paper represents an initial effort at policy description in the records area unduplicated by any other division in the Ministry of Community and Social Services.

No written policy governing verification of personal data has been developed by the Children's Services Division. Contrary to regulations and guidelines for adult social services, which permit broad verification

52 Macartney, Christine, (working draft for consideration of the Task Force), Safeguarding the Quality of the Case Management Recording System (Toronto: 1978) 1.

of information to prevent welfare fraud, unwritten policies for children's services generally favour a belief in original record sources. The former policy may invade privacy by requiring evidence of many personally sensitive details of a client's life, but may reduce errors; the latter policy is not initially intrusive but endangers privacy by encouraging the cataloguing of subjective judgments and possibly incorrect data.

Varied and inconsistent practices by system, agency and program reflect the dearth of policy regarding information collection and verification. Clients are usually referred to particular Children's Services agencies by other public or private service agencies, schools, doctors, courts or parents. Initial intake procedures almost always include parents or legal guardians, who are personally interviewed with the child by a social worker or records manager at the agency. During the interview, the guardians are usually asked to relate their perceptions of their child's problem. Institutions and Children's Aid Societies generally employ the services of various professionals such as medical doctors, psychologists, psychiatrists, speech therapists and counsellors to assess the incoming child's and his/her family's problems. Many of these assessments entail long hours of interviews and testing for the child and family, who often reveal very personally sensitive information which becomes part of a case record. Refusal to give information is rare and generally does not result in termination of service.

Other programs collect data by very different methods. The Child Abuse Program and Children's Aid Societies dealing with child abuse receive complaints by telephone or mail from neighbours, relatives, doctors and sometimes the victim him/herself about alleged acts of abuse or neglect. The complaint is recorded, whether or not it is verified or justified, and is followed by a visit to the child's home and sometimes the homes of neighbours, where accounts are recorded and evidence documented. Information gathered by the CAS worker investigating the case may or may not be sent to the Ministry Child Abuse Program in Toronto, depending on particular attitudes and practices within the individual societies. If the occupants of the homes investigated refuse to give information, the CAS has no legal power to pursue the matter except by recommending that the child be taken into foster care and/or by placing charges, which automatically result in a court hearing within five days. At that point, a judge may subpoena and demand the testimony of parents and others involved.

Children's Aid Societies collect and file a variety of objective and subjective data about prospective and active foster parents, gathered in regular visits to foster homes. This data may include criminal records (verified by police), personal habits, religious beliefs and practices, and perceived attitudes and actions toward children in care. One computerized periodic foster home evaluation includes 27 questions assessing foster parents' abilities, for example, to "demonstrate that they are caring persons who can meet the needs of a child with warmth and understanding," and to "demonstrate an ability to accept the rights,

responsibilities and obligations of the society in respect to each child in its care."

Day Nurseries programs gather all data about incoming children and their families in personal interviews at municipal offices and the nurseries themselves. The financial form completed for parents requesting subsidies is as detailed as applications for general welfare assistance and may require verification of income, assets and budgetary items. Parents who find such questions contentious and refuse to reveal information may be refused service.

c) Record Storage

No Division-wide written policy addresses the subjects of physical record security maintenance or destruction, although the Consultation Paper on Information Systems Development recommends that "client identifiable clinical information should be maintained in paper records only, in a secure location."⁵³ Only the Corrections Branch, which places a high value on data security, has issued written standards applicable to all its institutions, stating in part:

At the institutions, confidential files are under the care and control of a designated person. They are kept in locked cabinets and are drawn by authorized personnel by signature in a file control book, file control card, or "out" file cards.

53 Children's Services Division, op.cit., 36.

The details of file control for each institution are incorporated into the institution standing orders. 54

Agencies and institutions operating under the Children's Mental Health Services Branch follow record security policies set up by the Ministry of Health, which include logging in documents, locking record files at night, and allowing only trained records personnel access to personal records.

In terms of identity protection, the Mental Health Services Branch has the strictest policy, generally setting up files by case numbers (which are cross-indexed by name in a separate card file) or by unique code in its computer system. The Corrections Branch also advocates filing by case number, but indexes its computer systems by name of client. Generally, the Children's Services Division is moving toward strict principles of identity protection in automated case files which will prohibit any identification in clinical information systems and limit other computer files to minimum case identification by unique code.⁵⁵

In regard to file maintenance and destruction, no regular schedule has been devised by the Division to ensure that personal records are destroyed or identification removed either at a certain time after service termination or when a child reaches the age of 18. No method

54 Ministry of Correctional Services, Standards and Procedures: Confidential Information (Toronto: June, 1976) A-7, 1.

55 Children's Division, op.cit., 36.

of data destruction has been specified. No direction has been issued on this subject despite the attitude on the part of management personnel interviewed that juveniles should be treated differently and separately from adults by the courts and other agencies.⁵⁶ It was strongly felt that the anonymity of juveniles should be maintained and that their actions as children should not count against them in adult courts or as recipients of adult services.

Data security, maintenance and destruction practices are inconsistent between central records areas and field locations, and among different agencies. Child Welfare files (including adoption records) held by the Ministry appeared to be extremely secure, locked in file drawers or large revolving file machines in rooms locked at night. The files are indexed by file number, and supervised by clerks who appear to have a high regard for the safety and confidentiality of personal records. All files taken out are logged by colour-coded charge-out slips. Data are regularly microfilmed, sensitive adoption records are transferred yearly to more secure records centers, and written records are destroyed

56 In a letter to the Commission dated January 5, 1979, the Ministry stated that "such inconsistencies that exist are due to the previous lack of co-ordination of Children's Services. Inconsistencies currently exist in all facets from funding to service to data collection. Therefore, it is unfortunately reasonable to assume that practices governing data security and privacy of information would also be inconsistent. The emphasis, however, should be on the efforts undertaken by Children's Services to correct the problems. The Division since its inception has identified the need for policies which both protect privacy of personal information and provide access to information by children who are the subjects of records."

by shredding six months after microfilming. All microfilmed records of child welfare cases since 1890 are retained permanently by the Branch in their personally identifiable, original formats.

While active, these same files may not be as well-secured by the 51 Children's Aid Societies which handle all child welfare cases. The Committee on Record Disclosure to Adoptees reported that:

Some adoptive parents expressed concern about having their personal records retained at certain local agencies, where it is felt that there may be a much too casual approach toward storage and safekeeping.

57

Security precautions vary by society and worker, some of whom keep unlocked files and take work to insecure areas. Identity protection through indexing, logging procedures, computer security, and time and mode of destruction of files also vary by society.

The active records of the Child Abuse program, which may contain allegations extremely harmful to subjects if revealed, are not protected when out of central Child Welfare files. A cabinet unlocked during the day in an open hall accessible to passers-by holds the records, which have sometimes been left on desks in open offices. Temporary staff have occasionally been utilized to transcribe and photocopy the files, which are identifiable by name and indexed alphabetically.

Corrections Branch manual records filed centrally with the Division are very well-secured and numerically indexed, but subject to more consistent security precautions than Child Welfare records at the field level, where standards set by the Ministry of Corrections are followed by training schools. Juvenile Probation record security, however, varies by individual office location. Although central records are coded three years after case termination, neither training school nor probation records are destroyed after case termination or when children reach 18, and files are reportedly sometimes passed to adult probation officers and adult courts.

Manual records held by the Corrections Branch may be more secure than computerized records, which are identifiable by name in both the Juvenile Information System and the Juvenile Probation System. Although the computer itself is strictly guarded, keypunch areas, access points for input, and rooms (where personally identifiable computer print-outs sit on desks) are open and readily accessible to unauthorized personnel. Also, the recent transfer of programs from the Ministry of Corrections to the Children's Services Division has resulted in occasionally misplaced forms and remaining storage in the former ministry. No records have been deleted from computer files since the inception of either system and no program has been developed to erase the records of those 18 or over.⁵⁸

58 In a letter to the Commission dated January 5, 1979, the Ministry stated that "A tender call has already been issued for a feasibility study into this whole data collection, data dissemination area. Children's Services Division has identified problems in this area and is attempting to correct them."

Mental Health Services Branch agencies and institutions adhere to a policy governing a medical model of record-keeping; all records are kept in a secure area, files are locked at night, forms are logged in and out, and indexing is by case number. Selected items of mental health records are compiled in the centralized Mental Health Statistical Information System (CMHSIS), which was designed to safeguard data integrity and data security. No identifiable names or addresses are recorded in computer files, which are protected by software including passwords and protocols and by extensive physical security on hardware.⁵⁹ In terms of records destruction, most mental health insitutions keep records permanently, some retaining old files in insecure areas such as basements and attics for over 20 years. One interviewee recalled an incident in which old records, left in a vacated house once used as a mental health group home, were discovered and taken by vandals.

Another program which handles some of the Division's most sensitive records has not followed the security precautions common to central records holdings. Although the Day Nurseries Information System keeps no personally identifiable files at the branch level, day nurseries and municipal offices which take subsidy applications keep income statements, medical information and other records of parents in all types of secure and insecure areas,⁶⁰ some locked and others not, throughout the

59 Children's Division, Mental Health Services Branch, Children's Mental Health Services Information System User Guide (Toronto: August, 1977) 1B - 1C.

60 Internal Memorandum, December 9, 1977.

province. Many types of personnel may have easy access to the forms, which are sometimes stored in desk drawers and rarely destroyed.

d) Transfer of Personal Information

No written policy governs transfer of personal information for the Children's Services Division as a whole, although policies are operative in some of its branches and programs which originated in other ministries. The majority of managerial personnel interviewed favour close restrictions; specifically client written consent for transfer of information from files held in the Division or by its contracted agencies. Regarding transfer into Division-held files from other agencies, or between Division agencies, most interviewees felt that the requesting agency should prove "need to know" prior to receiving any personal information. The "canons" for management of automated information systems proposed by the Consultation Paper for Information Systems Development reinforce this viewpoint for computer files, emphasizing that sensitive files be stored in paper form only and be made available only when necessary.⁶¹ While these canons are being translated into uniform policy, the Senior Policy Advisor for Systems has issued a memorandum directing all computerized systems managers to provide him with lists of persons requesting the receiving access to

61 Children's Services Division, op.cit., 36.

personally identifying data and to forward all future requests to him.⁶²

A problem surrounds the definition of "need to know." Some management level interviewees felt that qualification as a professional in the employ of the Ministry of Community and Social Services could obviate the necessity for client permission to transfer information and itself constitute a need to know. One interviewee stated:

The exception to client consent would be where one professional employed by an agency funded through the province asks for information from another professional who has seen the client in another agency funded by the province. I would assume that anyone employed by us would have high standards of confidentiality, wouldn't ask for the information unless he needed it, and would safeguard whatever he found out.

Others believed that standards of confidentiality differed among professionals, and that no transfer in any direction should take place without client knowledge and approval.

For all its institutions, the Children's Mental Health Services Branch maintains written policies on record transfer which originated in the Ministry of Health. These policies include screening of all telephone calls,⁶³ refusal to reveal personal information to unauthorized persons, and signed guardian consent to transfer any client information

62 Internal Memorandum, May 23, 1978.

63 Internal Memorandum, December 9, 1977.

among interested parties, such as from institution central records to school. With regard to age, children's parents or guardians are considered to be parts of client groups and files and therefore must give permission for release of information. Children over 16 years of age may be given some discretion in the matter.

Written standards for the Corrections Branch are more specific and more controlled than those governing other Branches.⁶⁴

64 Previously issued by the Ministry of Correctional Services, Standards and Procedures: Confidential Information (Toronto: June 1976) 1-10. The guidelines include:

- 1) Prohibition of conversations about institutionalized persons among institution personnel and non-institution personnel;
- 2) Advice "that it would be a breach of the Oath of Secrecy to surrender papers (correspondence, journals, diaries, books, articles, speeches, photographs and other memorabilia) to any authority without instruction from the appropriate Regional Administrator or the Director of Information;"
- 3) Directions to issue necessary information to requesting legal representatives or the police only after verifying calls, with the exception of release of address information, which may be given only with consent of the subject;
- 4) Specific procedures for dealing with requests for extensive personal information from various types of people and organizations, including the legislature, the media, and bill collection agencies;
- 5) Specific procedures for answering written enquiries for personal information, including special provisions for transferring reports made by clinical, social services or other professional staff, which may take place only with a signed consent by the subject, and if possible, the writer of the report;
- 6) Specific procedures for transferring reports to the Ombudsman, which must include a statement requesting "no further disclosure be made than is absolutely necessary to your purposes;"
- 7) Specific procedures for the transfer of pre-sentence reports.

Transfer of information about adoptees (held by the Child Welfare Branch) is governed by The Child Welfare Act, which states:

The papers used upon an application for an adoption order shall be sealed up and filed in the office of the court and shall not be open for inspection except upon an order of the court on the written direction of the Director [of Child Welfare]. 65

In contrast to the Mental Health Services and Corrections Branches and the Adoption Program, the Child Welfare Branch as a whole, the Child Abuse program, the Day Nurseries Branch and Observation/Detention Homes programs have no written policies governing personal record transfer. At present, conditions of transferral are contained in neither the contracts the Division signs with any of its over 600 serving agencies, nor any contracts for employment with Division personnel. However, the Children's Services Division has seriously disciplined and fired employees for releasing confidential information to outside parties.

Among the Children's Services Division records systems investigated, practices of record transfer and release vary considerably by program, agency and records supervisor or field worker interviewed. For example, methods of transfer may be by telephone, only in writing or only in person, and information may be sent by registered mail, regular mails, government mail, or courier. Strictly controlled systems like the Child Welfare files require requestors of information to present identification of their employ in a particular Branch and letters of permission from

65 The Child Welfare Act, R.S.O. 1970, s. 80(1).

Division officials, to wait while their identity is verified, to obtain client release and to sign out material taken. Less strictly controlled systems give material to anyone who says s/he is employed by the Ministry or any of its agencies (over 20,000 employees), without client release and without signing out files. Such divergent practices have occasionally resulted in misplaced files and unauthorized transfer of records to outside parties. Several examples were cited by records supervisors interviewed, including cases where employee divulged confidential information to friends, and biological parent information to adoptees. In one case, confidential information may have been used to blackmail parents with illegitimate children.

Table 5 summarizes information transfers between particular Children's Services programs or systems and three domains:

1) With other agencies and programs within or funded by the Ministry of Community and Social Services: A large number of exchanges take place with this domain; very few of them with client consent, either written or spoken. Exceptions occur between Children's Aid Societies and certain programs, especially Family Benefits, which issue adult public assistance. Some Children's Aid Societies are very reluctant to reveal any information to any other agency or program without the signed consent of the client and a letter from the Director of Child Welfare. At the same time, Societies request and receive large volumes of information from other Ministry programs and agencies.

TABLE VIII.5

INFORMATION TRANSFERS BETWEEN SELECTED
CHILDRENS SERVICES AND THREE DOMAINS

| Program | CHILD WELFARE | CORRECTIONS |
|---|--|--|
| Selected Types of Record Subjects | <ul style="list-style-type: none"> a) CAS Clients b) Adoptees and Their Families c) Foster Parents d) Abused Children e) Alleged Child Abusers | <ul style="list-style-type: none"> a) Wards b) Training School Residents (JIS)* c) Probationers (JPS)* <p>* also included in Wards files</p> |
| 1) Between Program and other agencies, programs UNDER MINISTRY | <ul style="list-style-type: none"> . local Children's Aid Societies . Branch personnel . Family Benefits workers . residences, institutions | <ul style="list-style-type: none"> . training schools . probation officers (including adult services) . Children's Aid Societies . Training Schools Advisory Board . regional offices and managerial personnel . Family Benefits, other public assistance programs |
| 2) Between Program and agencies, programs, UNDER OTHER ONTARIO MINISTRIES, AGENCIES, LOCAL GOVERNMENT | <ul style="list-style-type: none"> . Ministry of Education and local schools . police . courts (only with subpoena) . Registrar General . OHIP . politicians (with consent) . hospitals, Public Health (witnesses of abuse) . Child Abuse Task Force and local treatment teams | <ul style="list-style-type: none"> . Ministry of Education and local schools . police . courts . Ministry of Corrections . OHIP . politicians (with consent) |
| 3) Between Program and organizations PEOPLE OUTSIDE GOVERNMENT | <ul style="list-style-type: none"> . doctors, psychologists . private social service agencies . lawyers . prospective adoptive parents . alleged child abusers (proposed) . politicians (with consent) . neighbours (witnesses of abuse) | <ul style="list-style-type: none"> . doctors, psychologists . private social service agencies . lawyers . ministers, other character references . media (only with consent) . politicians (with consent) - No transfer from computerized systems |

TABLE VIII.5 (Cont'd ... 2)

| Program | MENTAL HEALTH SERVICES | DAY NURSERIES |
|--|--|--|
| Selected Types of Record Subjects | a) Mental Health Patients b) Thistletown Patients* * also included in Ministry CMHSIS system | a) Day Care Children and Families |
| 1) Between Program and other agencies, programs UNDER MINISTRY | <ul style="list-style-type: none"> . regional offices and managerial personnel . other treatment centres receiving client (with consent) . FBA workers . Children's Aid Societies - No transfer from CMHSIS | <ul style="list-style-type: none"> . FBA workers . other public assistance programs . Community Service Centres |
| 2) Between Program and agencies, programs UNDER OTHER ONTARIO MINISTRIES, AGENCIES, LOCAL GOVERNMENT | <ul style="list-style-type: none"> . courts (only with subpoena) . hospitals (with consent) . Ministry of Education at local school level (with consent) . Public Health - No transfer from CMHSIS | <ul style="list-style-type: none"> . municipally-run day care centres . police |
| 3) Between Program and organizations PEOPLE OUTSIDE GOVERNMENT | <ul style="list-style-type: none"> . lawyers (through legal services) . media (only with consent) . private medical practitioners . private social service agencies - No transfer from CMHSIS | <ul style="list-style-type: none"> . day care centres, nurseries, private home day care parent . family doctors . banks, other financial institutions . employers . landlords |

2) With agencies and programs within other Ontario ministries, their funded agencies or local governments: The overlap among various types of social services and protective services promotes large and constant information exchanges. Educational data is transferred without client consent except by some Mental Health Services institutions. OHIP, hospitals and public health agents of the Ministry of Health regularly give and receive information, some of which (specifically OHIP information) is stored in Ministry of Health computer files. The police are likely to receive information from any program only after presenting identification and revealing reason. If Day Nurseries subsidy programs suspect fraud, files may be handed over to police by municipal agencies. Children's Aid Societies and Mental Health institutions are unlikely to give the courts any information about clients without subpoena. On the other hand, Corrections programs regularly exchange information with courts, and in some cases, information on juveniles is reportedly provided to adult courts. Statute and regulations require the transfer of detailed pre-sentence reports to court officials and both prosecuting and defending attorneys. Further dissemination of this information to other parties occurs frequently, sometimes through the carelessness of pre-sentence report recipients, who have reportedly left documents in washrooms and other public places.

3) With organizations and people outside government: Private medical practitioners and psychologists are the most frequent contributors of information from this domain to program client files, usually with verbal client consent but without the client's full awareness as many times

s/he does not see medical reports before they are transferred. Politicians, lawyers, ministers and private social service agencies acting in the client's interest and with the client's consent are able to obtain information from personal files or contribute information, such as letters of reference, to client files. No abuses of this practice were reported by interviewees.

However, interviews revealed one former practice, in which sensitive identifiable client information from a computer system was revealed to a private social service watchdog agency interested in tracking mental health patients in its area. This wholesale transfer of data without client consent was stopped because of potential misuse of the data.

The most regularized transfer of client information from the private sector takes place in the Day Nurseries program, which requires financial and other data from banks, insurance companies, pension plans, employers and landlords to determine eligibility for subsidy. Client consent utilized to obtain this information varies by jurisdiction. Metro Toronto uses a blanket form with no specific sources named. The types of information transferred are particularly contentious to parent applicants, who have complained that their known status as subsidy applicants or recipients may affect their borrowing power with banks and their reputations with employers and landlords, and that the practice of transfer introduces the possibility of uncontrolled dissemination of personal data to others. One case of unauthorized dissemination of information was reported by an interviewee at the management level, who

received a complaint from a professional whose status as a subsidy recipient was revealed by day-care program managers to outside private parties.

e) Research Access

Written policy regarding access to and use of personal records by researchers has not been issued for the Division as a whole, but has been carefully formulated and adhered to by all branches and most programs. All but one program surveyed stipulates that research proposals must be approved by the Director of the program and that researchers must sign an oath of confidentiality, guaranteeing anonymity of subjects and secrecy of records. The Metro Toronto Day Nurseries program requires no formal submission of research plans and no personal guarantee of confidentiality, but does require signed consent of parents for research involving their children. Signed consent of participating subjects is not required by most other programs.

The most comprehensive research standards have been utilized by Corrections programs, which follow policy issued by the Ministry of Corrections in 1976. This policy allows only research projects which have been approved by that Ministry's Research Advisory Committee. The Committee judges the project's ability to meet certain criteria, which include the safeguarding of client privacy, voluntary participation by subjects, and beneficial use of results. All researchers must present

their qualifications and sign an oath of secrecy.⁶⁶ Although former Corrections employees now working for the Ministry of Community and Social Services generally adhere to this policy, many interviewees were uncertain whether the old policy should be applied to research decisions now made in Children's Services Division.

f) Subject Access to Personal Records

Policy governing access to a personal record by the subject of that record has not been developed by the Children's Services Division. Attitudes of interviewees were much more favourably disposed toward subject access than those surveyed in adult services. Without exception, management level interviewees in Children's Services felt that children and their families should be able to see their files and to register disagreements with file contents. In regard to reports prepared by third parties, such as psychologists and family physicians, many interviewees believed that the signed consent of the report writer should be obtained before allowing the subject to see that portion of the file. In some cases, obtaining that consent was seen as a problem, especially when clinicians viewed their judgments and reasons for judgments as possibly detrimental to the child, as related in an example by one interviewee:

66 Ministry of Correctional Services, Policy Concerning Submission of Research Proposals To Be Conducted Within This Ministry (Toronto: December, 1976) 1-5.

What if the child had been sexually abused by the father and in the clinician's viewpoint, the abuse had seriously affected her psychological condition, but the child and father have a healthy relationship now? Seeing that history in black and white might cause the child irreparable harm.

Another problem foreseen in allowing subject access was the presence of family case files, which contain information about parents and others significantly involved in a child's life. Some interviewees thought that all those whose records appear on a file should be notified of potential subject access at the time of information gathering (i.e. at initial interview). Others felt that such notification is insufficient protection and that references to people other than the subject should be removed before access is allowed.

A third problem related to client access has been examined by the Committee on Record Disclosure to Adoptees. In adoption cases, the protection of both child and third parties has been viewed as particularly important. The Committee noted that adoptive parents fear harrassment or changed affections of their adoptees by natural parents. Some professionals feel explicit knowledge of or reunions with biological parents could severely harm adoptive children. In reviewing public briefs and literature on the subject, including evaluations of information exchanges in several American states and other foreign countries, the Committee found no evidence of damage or backlash to any party as the result of releasing biological parent information or identities to adoptees, or adoptive family identities to biological parents. Most adoptees appear to have benefited from the experience. Accordingly,

the Committee recommended the formation of an Adoption Registry administered by a trained mediator, to assist adoptive children over 18 years of age, adoptive parents and biological parents in obtaining (or preventing) the release of information and reunions of affected parties.⁶⁷

A fourth problem surrounding policy in this area entails defining age of exclusive access. Some children may wish to view their files without their parents' presence, especially if information about a sensitive matter such as birth control is contained within. Although 16 was often mentioned as a good age to allow exclusive access, several interviewees thought that younger children, if mature, should be able to exclude parents from viewing records.

Client viewpoint about access to files has been assessed by the Youth Services Network of Metropolitan Toronto. Under contract to the Division of Children's Services, the network personally interviewed approximately 60 present and former clients of 35 youth service

67 Children's Services Division, Report of the Committee on Record Disclosures to Adoptees, op.cit., 7-25. The new Child Welfare Act, which came into force June 15, 1979, incorporated some of the Committee's recommendations by setting up the Adoption Disclosure Registry. Under s. 81, both adoptees over the age of 18 and biological parents who gave up children for adoption may register their names and wishes regarding information with local Children's Aid Societies or the Child Welfare Branch. In the event of a match between registered adoptees and natural parents, and the adoptive parents' permission, the two sets of registrants may meet. If adoptive parent permission is denied, the Director of Child Welfare may exercise discretion in the case.

organizations in the spring of 1978. All those interviewed believed that files should be opened to subjects. Reasons for favouring access included:

- 1) A sense of ownership of the information, "It's about me, so I deserve to see it."
- 2) A belief in personal file access as a "basic right" for everyone.
- 3) The possibility of learning from the file in order to improve behaviour and to participate in the decision-making process, "I want to see how far I've come, and how much more I have to go."
- 4) The opportunity to check records for accuracy and challenge possible errors.

On related issues, a majority of children's services clients believed that they should be present in all courtroom situations and be given more opportunities to participate in decision-making about their future.⁶⁸

In contrast to present practice in adult services, many Children's Services clients and former clients have been allowed and encouraged to see their files. Residents of certain institutions and group homes have regularly reviewed file contents (including daily logs prepared by child workers) as part of the therapeutic experience, and in one interviewee's words, "as part of getting control of their lives, learning to take responsibility for their actions." Some institutions now make it a regular practice to include the child and his/her parents in

68 Youth Services Network of Metropolitan Toronto, What are you Doing? Nothing! Where are you Going? Nowhere! (Toronto: April 18, 1978) pages unnumbered.

periodic case reviews, with reportedly "excellent" results. No negative experiences as a result of opening or viewing files were known by interviewees.

Several present and former Children's Aid Society wards and some adoptive children have been able to obtain information about their pasts, either by personally viewing records in the presence of a social worker, or by reading summary letters prepared with the authorization of the Director of Child Welfare. To the knowledge of both management and field level interviewees, no damage to clients or to other persons mentioned in records accessed had occurred.

Of the approximately 40% of Childrens Services clients who have appeared in court, a large majority have been present during entire court proceedings, not only hearing all evidence in the case, but also being afforded the chance to challenge statements and judgments made about them.⁶⁹ Those represented by lawyers have often seen or been given a copy of detailed pre-sentence reports, which usually contain reference to family histories and several third party assessments. Again, no interviewees knew of negative experiences, such as physical assault or harrassment of third parties or psychological trauma of the client, induced by such open procedures.

69 Ibid.

C. Impact of Computerization on Privacy
in Social Service Record-Keeping

Social service records have not been computerized to the same extent or sophistication as health or law enforcement records examined in the course of this research. Nevertheless, the trend toward automation of personally identifiable social service records has markedly increased since the mid-1970's, when several systems were introduced. In addition to those implemented since that time, management level interviewees of the Ministry of Community and Social Services reported plans for two new systems which will be operative within a year. When these are completed, almost all manual social service record systems will be at least partially computerized or capable of easy conversion based on model systems which have already been tested. Table 6 summarizes the history and salient characteristics of eight of these systems.

The most striking feature of all the systems investigated is the complete overlap of manual and computerized files. Many automated systems in government and business have eliminated copious manual data collection and storage. However, the computerization of Ontario social service records has not resulted in the elimination or replacement of extensive manual record collections. In some cases, duplication exists within the Ministry; in other cases, between the Ministry and the service provider. In fact, manual files have increased in volume with the addition of each new computer system form. For example, copies of up to ten computer forms detailing Vocational Rehabilitation Services

status are stapled to already large case files which contain the same information in much more detailed form.

This overlap significantly affects privacy issues. While public attention has focused on the security of proliferating computer systems, the most obvious security problems which occur in existing manual systems, containing much more detailed and sensitive information, have been overlooked. For example, a brief presented to the Commission outlines a hypothetical case in which a mother pays an inherited sum of money to a computer programmer to access computerized data about her child placed in a foster home.⁷⁰ The brief neglects to state that in actuality, to find out any information about the child from the computer system, the programmer would have to unlock a heavy steel door, unlock a heavy steel safe, find one (of several) disks containing the case-numbered record, utilize the proper system protocols to activate the system, run through thousands of case records, recognize the right address (the mother does not know the child's name), and understand a complicated coding system. On the other hand, it is conceivable that the mother herself might be able to discover extremely sensitive information about the child merely by presenting a false ministry identification card to any of several holders of manual information.

70 Staff Association of Metropolitan Toronto Children's Aid Society, A Brief to the Commission on Freedom of Information and Individual Privacy (Toronto: February, 1978) 18.

TABLE VIII.6

CHARACTERISTICS OF COMPUTERIZED PERSONAL
RECORD SYSTEMS IN THE SOCIAL SERVICES

| Program (Name of Computerized System) | VOCATIONAL REHABILITATION Rehabilitation Information System (RIS) | FAMILY BENEFITS Ontario Allowance Program (ONTAP) | | GENERAL WELFARE Municipal Assistance Information Network (MAIN) | MENTAL RETARDATION Resident Statistical System (RSS) |
|--|--|--|-------------------|--|---|
| Year Introduced | 1976 | 1973 ⁺ | | 1977 ⁺ | 1977 |
| Manual Data Overlap | Complete | Complete | | Complete | Complete |
| Client Made Aware | No | No | | No | No |
| Identifiable by Name | Yes | Yes | | Yes | No ^x |
| S.I.N. Collected | Yes | Yes | | Yes | Yes |
| Subjective Data Collected | Yes | No | | No | Yes |
| Transfer of Information | | (Type A) | (Type B) | | |
| ORIGIN | Field Offices | Prov.Ben.Br. (Eligibility Analysis & Section) | Field Terminal | Municipal Terminal | Residences |
| EDIT/CORRECT | System Office (Hepburn Building) | Prov.Ben.Br. (Automation Services Section) | Field Worker | Municipal Terminal | Ministry of Government Services Building |
| UPDATE | Field Offices | Prov.Ben.Br. (Automation Services Section) | Field Terminal | Municipal Terminal | Ministry of Government Services Building |
| COMPILATION | System Office (Hepburn Building) | Prov.Ben.Br. (Automation Services Section) | Unnecessary | Unnecessary | ComSoc Accounts Br. (Hepburn Building)* |
| KEYPUNCH | Keypunch Room (Hepburn Building) | Prov.Ben.Br. (Automation Services Section) | Unnecessary | Unnecessary | ComSoc Accounts Br. (Hepburn Building)* |
| INPUT AT: | Terminal Room (Hepburn Building) | Prov.Ben.Br. (Automation Services Section) | Field Terminal | Municipal Terminal | Government Building (880 Bay) |
| TO: | QPCC | QPCC | QPCC | QPCC | QPCC |

+ Not fully implemented

⊕ District Offices send data in rough
manual form to Eligibility Analysis
Section, where data transferred to
ONTAP forms.

x Only first letter of first name and
first two letters of last name used.

* Backup copy kept for federal BILLCAP
system.

TABLE VIII.6 (Cont'd ... 2)

| Program (Name of Computerized System) | MENTAL HEALTH Children's Mental Health Statistical Information System (CMHSIS) | CORRECTIONS Juvenile Information System (JIS) | CORRECTIONS Juvenile Probation System (JPS) | CHILD WELFARE Case Management Information Systems for Children's Aid Societies (e.g., Metro Toronto CAS) |
|--|---|---|---|---|
| Year Introduced | 1977 | 1974 | 1977 | 1978 ⁺ |
| Manual Data Overlap | Complete | Complete | Complete | Complete |
| Client Made Aware | In some cases | No | No | No |
| Identifiable by Name | No ^x | Yes | Yes | Yes |
| S.I.N. Collected | No | No | No | Yes |
| Subjective Data Collected | No | Yes | Yes | Yes |
| Transfer of Information | | | | |
| ORIGIN | Child Mental Health Centres | Training Schools | Probation Offices | CAS Field Worker |
| EDIT/CORRECT | Child Mental Health Centres | Wards Records (700 Bay) | Wards Records (700 Bay) | CAS Systems Room |
| UPDATE | Child Mental Health Centres | Training Schools | Probation Offices | CAS Field Worker |
| COMPILATION | Child Mental Health Centres | Wards Records (700 Bay) | Wards Records (700 Bay) | CAS Systems Room |
| KEYPUNCH | QPOC | Accounts Branch (Hepburn Building) | Accounts Branch (Hepburn Building) | CAS Keypunch Room |
| INPUT AT: | QPOC | Terminal in MacDonald Building | Terminal in MacDonald Building | CAS Computer Room |
| TO: | QPOC | QPOC | QPOC | University of Toronto Computer |

+ Not fully implemented

@ District Offices send data in rough manual form to Eligibility Analysis Section, where data transferred to ONTAP forms.

x Only first letter of first name and first two letters of last name used.

* Backup copy kept for federal BILLCAP system.

Nevertheless, the impact of computerizing social service records on a large scale cannot be underestimated. As noted in chapter IV, automating records magnifies and multiplies difficulties in protecting the privacy and confidentiality of record subjects. According to some management level and field personnel interviewed, these difficulties have only been considered cursorily, if at all, in planning computerized record systems for the social services. The results of this lack of attention are systems which appear to invade the privacy of subjects and to inconsistently and inadequately secure personally identifiable data. The most serious factors contributing to privacy and security problems are discussed below, organized according to stages in record processing, and summarized in Table 6.

1. Data Collection

a) Client Awareness of Computerization

None of the systems examined has required that subjects be notified of their inclusion in a computerized information bank, either when data is initially collected or at regular intervals when information is updated. Fieldwork and records personnel interviewed had in general not informed record subjects of the existence of computerized systems, asked subjects' permission for transmittal of manually-collected information to such systems, or requested that computerized records be checked by subjects

for accuracy and completeness. One interviewee reflected the common viewpoint on this subject:

Well, no, we don't ask them whether or not we can put the records on a computer, I doubt if anyone even knows we do it. They might object, and then what would we do?

An exception to this attitude was revealed by one interviewee. Trainees in the use of CMHSIS (Children's Mental Health Statistical Information System) were at one point instructed to inform subjects of the new system. When one intake worker did describe the system to incoming clients, a few reportedly objected, asking that their records not be computerized. With permission of a supervisor, no records of the objecting clients were processed for automation. Most social service clients have not had the option of refusal, and no ministry policy has been issued to handle the situation.

b) Collection of Subjective Data

Tables 1 and 4 include references to subjective data of all types which are collected from social services clients. Much of these data are included in computerized information banks, as noted in Table 6. Computerized subjective data are even more invasive of privacy than manually-recorded subjective data, for three reasons. First, the information is highly judgmental, depending completely for its accuracy on interpretation of actions or behaviour by one counsellor or intake worker. It is therefore unreliable and error-prone, but in manual

form can at least be easily attributed to the person writing the report, and backed up by documentary evidence. Once computerized into an anonymous standardized format, recorder accountability and documentation are lost. It becomes very easy to say, "But, the computer said" Examples of unsigned, undocumented subjective statements which are printed in computerized format include two from the Rehabilitation Information System:

1321 IS ANXIOUS AT WORK, RESTLESS, HAS DIFFICULTY TAKING WRITTEN INSTRUCTIONS. IS DEPRESSED, HAS LIMITED SOCIAL CONTACTS, LACKS CONFIDENCE IN WORK SKILLS, TAKES FREQUENT BREAKS.

1321 PERFORMANCE IS IMPAIRED BY ANXIETY, QUICK DISCOURAGEMENT AND SELF CRITICAL ATTITUDES. SHE BECOMES EMOTIONALLY UPSET WHEN UNDER PRESSURE AND THIS TRIGGERS SEIZURE. 71

Secondly, without the documentation in a manual file, computerized subjective information may present a very inadequate and distorted picture of a client. Adding to this problem, those accessing a computer file may often see whatever data elements are desired, without observing related variables. Explicit, incomplete codes for subjective data were found in many computerized social service record systems examined. For example, the Juvenile Information System records only "yes/no" answers for eight categories of scars, marks, disabilities, including "physical defects" and "carvings."

An even more contentious example: one of the Metro Toronto Children's Aid Society's computer systems records worker assessment of 42 subjective

factors in a diagnostic profile, according to four codes "major strength," "minor strength," "major weakness" and "minor weakness." These factors include: ability to manage affairs; anti-social behaviour; interpersonal relationships between parent/partner; and sexual adjustment of child.

A third danger of automating subjective personal data is the aura of permanence such data assume once stored in computer files. The opinion of a field worker or counsellor is likely to change during the period of treatment or service. Such changes are recorded in field notes or interview notes completed manually after every contact with a client. However, those changes are disregarded in computer systems, which usually require assessments of subjective data categories only at intake (and sometimes at termination). While objective categories such as address are updated and corrected, the motivation, attitudes and other subjective traits of clients remain unchanged in computer printouts.

c) Collection of Social Insurance Number

Like other programs in Ontario (see Chapter V), social service programs and agencies have promoted the use of standard identifying numbers for computerized record systems, specifically the Social Insurance Number. As noted in Table 6, five of the eight systems examined collect and store the number. Systems managers interviewed revealed some concern about the widespread collection of the Social Insurance Number, which theoretically may be used to link information among many systems. They

generally felt that Ministry technology was not sophisticated enough to enable linkage by the number, and that "no one would be interested in finding out about our clients anyway."

2. Preparation of Data for Computerization

Unlike manual data, machine-readable data generally undergoes several preparatory steps before input to a computerized record system: editing/correcting, updating, compilation, and keypunching. Although every step may improve the accuracy and completeness of the data, every step allocated to different personnel in different locations also increases the likelihood of error, loss and misuse.⁷² One systems manager described the ministry's efforts to computerize as much information as possible as a "Ben Hur project approach, involving a cast of thousands."

a) Editing/Correcting

In the course of our research, it became clear that social services field staff charged with completing forms for computerized systems sometimes resent transferring manual data to the forms. Interviewees

⁷² Two of the more sophisticated systems now partially implemented, ONTAP and MAIN, avoid these possibly privacy-invasive steps by utilizing field terminals and simultaneous self-edit programs connected directly to the Queen's Park Computing Center.

stated their disapproval of computerization, not because of client privacy considerations but because of the duplication of work, their lack of involvement in system design, protectiveness toward what they regard as their own records, as well as suspicion of management goals. Although clearly not within the scope of this investigation, management-staff relations appear to influence significantly computer form errors. One computer records clerk reiterated the problem:

The field workers don't care about the accuracy of forms they hand me for editing. As far as they're concerned, the computer was just thrown at them and they have to fill out twice as many forms because of it. So they do it as quickly as possible and count on me to look them over carefully.

All computer records clerks and systems managers interviewed find a high percentage of errors on forms they review, which therefore must be returned to the originating worker or corrected by telephone. As noted in Table 6, corrections and editing almost always take place in a different location from the one where forms are initially completed. Forms are transported by hand, regular mail, government mail, registered mail, government courier or private courier, with little consistent regard for security of data. Consequently, several systems reported occasional loss and misplacement of forms. Every transfer and telephone communication endangers the confidential client-worker relationship without the client's knowledge.

b) Updating

Frequency of updating client status in computerized files varies from daily to monthly, with most systems requiring updates when client status actually changes at the field level.⁷³ Because computer personnel usually have no idea of client movement, the timeliness and correctness of updates are difficult to determine. All systems managers interviewed related problems in this area, such as:

Sometimes a termination form will come in for a client we don't have listed as intaken yet, or an address change will come in from an old address the computer never received any information about.

Time lags and mistakes in updating information are most likely to endanger the privacy and confidentiality of clients and data when administrative personnel utilize computer-generated data for decision-making. Family Benefits workers, for example, pointed out that incorrect decisions regarding eligibility from the Provincial Benefits Branch were sometimes based on faulty or incomplete computer information updates submitted by the workers themselves. Even when not utilized for decision-making, untimely and incorrectly updated information endangers confidentiality if it is disseminated in personal form to third parties, such as program district managers.

73 The most sophisticated systems, MAIN and ONTAP, provide facilities and procedures for the most frequent client-status updating.

c) Compilation

At any of several points in preparation for computer entry, but usually before keypunching, manually-completed forms are gathered from outlying locations and compiled. Some systems include strict procedures for recounting and numbering forms at each point and storing forms in secure places. Other systems never count forms and system clerks leave personally identifiable forms on desks in open areas while awaiting keypunching. The latter methods of compilation not only increase the risk of loss and misplacement, but also expose personally identifiable data to unauthorized personnel who may betray client confidentiality.

d) Keypunching

Keypunchers handling personal data forms for computerization are in many cases unaware of the sensitivity of information they process. For example, one keypunch supervisor interviewed was surprised at questions relating to the confidentiality of personally identifiable data about patients in institutions for the mentally retarded. She regularly received special instructions to recount and safeguard forms for keypunching to a computerized employee payroll system, but had never been instructed to take any precautions to protect the client data. A few systems employ keypunchers on a contractual basis in times of overload, some of whom are not required to take secrecy oaths and who may not be as mindful of data confidentiality as permanent employees.

After keypunching, forms are again treated inconsistently. They may be returned to a field location, kept for reference in a central location, or destroyed, sometimes by shredding, other times by discarding into a convenient wastebasket.

3. Computer Input, Storage and Output

Once the manually-collected, edited, updated, compiled and keypunched information is in a machine-readable form on cards, it is generally transferred (usually hand-carried) to a terminal area or to a computer processing centre where it is handled by programmers and by general systems personnel. The exceptions to this rule are some ONTAP (Family Benefits) and MAIN (Municipal Social Services) data, which are input at experimental field locations by remote terminal, and case management information systems of Children's Aid Societies, which either have their own small computers or input data by remote terminal to university computers.

Lapses in security at this stage of computer processing pose serious threats to client privacy, which could be endangered by unauthorized retrieval and misuse of personally identifiable, sensitive and often historical computerized files. If more than one record system were stored in the same computer area, and if precautions were inadequate, that data could be combined to form a profile of a client who used several social services. Three types of precautions taken to counteract these dangers were investigated.

a) Authorization of Personnel

All salaried employees with access to computer rooms in Queen's Park must be authorized and must present identification. However, consultants employed on a contractual basis often work directly with data and with certain systems examined. The problem of high turnover rates of consultants with the expertise to operate systems has been recognized by Ministry of Community and Social Services management. This problem is partially addressed in purchase-of-service contracts, which contain the clause, "the security and confidentiality of information received by the supplier during the course of the assignment must be guaranteed."⁷⁴ In field locations and agencies, where the few people with access to computer terminals or small computers recognize each other, personnel authorization is not a problem.

b) Physical Security

A factor closely intertwined with personnel authorization is physical security of the building and room which house the terminal or computer. Although security appeared to be more than adequate at the Queen's Park

74 Internal Memorandum, Financial and Administrative Services Division, December 1977. In a letter to the Commission dated January 5, 1979, the Ministry stated that "Because of the potential problems regarding the use of external consultants, the Ministry is trying to increase the number of in-house permanent staff and thus reduce reliance on consultants."

Computer Centre, outlying social agency buildings and computer rooms are often unlocked and sometimes unattended.⁷⁵ A December 1977 internal memorandum authored by a member of the Ministry's Management and Financial Services Branch also expressed concern about easy access to certain government buildings containing terminals; in particular, one where

After hours, the security procedures in the building are almost non-existent and in fact make a mockery of all our other efforts to restrict access to confidential information. 76

By July 1978, the problems in physical security of that building had not been corrected to the satisfaction of systems personnel interviewed.

c) Computer Security

Beyond protection of physical access to a building or room, the computer itself and the system usually control access to files. As explained in Chapter IV, these controls include passwords, secret account numbers and user codes, system protocols, audit trails and transaction files. Some of the systems examined utilize far more controls than others containing equally sensitive personal data, indicating a lack of standards

75 One program, Family Benefits, has attempted to correct this problem by issuing new terms for installation of the QNTAP system, which require that all terminals be located in secure locked rooms.

76 Internal Memorandum, Financial and Administrative Services Division, op.cit.

for computer security in the Ministry. The recommendations of technical reviews of security and controls in ministry-held computer systems, conducted for the Management and Financial Services Branch in 1977 (not revealed to the Commission) are, according to some interviewees, being implemented at a pace which many system managers feel is too slow.

4. Distribution of Computer Generated Data

The output of social service computer systems almost always includes computer-printed lists of clients and status changes, either as a check for field workers, system managers, and supervisory personnel or as a management tool for program planners and evaluators. Most systems which input personally identifiable data -- only CMHSIS (Children's Mental Health Statistical Information System) and RSS (Residential Statistical System) are exceptions -- also output personally identifiable data in this form. Print-outs are regularly copied and transferred to authorized personnel in field locations and in district and central ministry offices, by the same inconsistently secure means used to transport manual forms to computer locations. Some systems personnel interviewed were not sure what constituted authorization, and kept no list of outgoing print-outs. Both before and after transport to field users, personally identifiable print-outs are sometimes piled on desks in visible and accessible areas, and taken to meetings which unauthorized personnel and non-government employees attend. Several systems managers interviewed are concerned that personally identifiable computer print-

outs containing sensitive information have been found on top of locked filing cabinets containing the same records in manual form. A recent request for named computer files of juveniles attending training schools from an outside police-connected agency, highlighted the lack of rigid controls on the distribution of computerized data in the Children's Services Division, and prompted a detailed policy statement by management correcting the matter.⁷⁷ Not all divisions and programs have similarly addressed the problem.

5. Trend Toward Integration of Computer Systems

One factor related to all the above is integration of formerly separate computer systems which contain different pieces of data about the same clients or potential clients. From the viewpoint of client privacy, the most important attributes of integration are the ability to formulate a client profile and create new data elements without the knowledge of client subjects. These attributes are explained more fully in Chapter IV. The following hypothetical example of social service system integration may emphasize its serious implications.

Let us suppose that all adult social service personal data banks held by the Ministry of Community and Social Services are integrated in their present form.⁷⁸ A counsellor wishing to

77 Internal Memorandum regarding Security of Automated Information Systems, May 23, 1978.

78 Present Ministry policy prohibits linkage between systems which identify Children's Services Division clients and other Ministry or outside programs.

make a treatment decision about an applicant to a Vocational Rehabilitation program searches computer systems for information, rather than ask the applicant himself. From ONTAP, he finds that the applicant's mother receives Family Benefits for deserted wives and that the applicant is an illegitimate child; from MAIN, he finds that the applicant's family has received municipal welfare assistance in two municipalities; and from the Rehabilitation Information System (RIS), he finds that one of the applicant's sisters was evaluated as an "unmotivated" Vocational Rehabilitation client receiving treatment for drug addiction. Concluding that the applicant is a poor risk and because of his background is unlikely to achieve in the program, the counsellor refuses to admit the applicant for treatment. Moreover, this judgment is fed into the integrated system, and the applicant is "blacklisted" by other provincial social service programs. Three years later, when applying for a building maintenance position with the province, he is rejected by the Department Head, who has obtained unauthorized computer listings confusing him with his sister from the integrated system.

Both management and system personnel interviewed discussed two model systems already integrated and plans for the integration of several other existing systems. When issuing Family Benefits checks, the present ONTAP system already searches its own records and General Welfare Assistance payment files to find out whether any client is receiving assistance from both programs or from more than one jurisdiction. Four pilot municipal systems now have the capacity to integrate data about clients in several provincially-funded social service programs, including General Welfare Assistance, Home Care Services, Day Care, Senior Citizens programs and one non-ministry funded program, i.e., housing services. The linked systems search files for registration of clients with the same name and birthdate in participating jurisdictions.

According to several interviewees, proposals to integrate all computerized income maintenance programs administered or funded by the Ministry, which include Family Benefits, General Welfare Assistance, Vocational Rehabilitation, and Guaranteed Annual Income Systems, have been discussed among senior administrators. One interviewee at the management level favouring such a system feels it is justifiable

... because of the flow of clients from one program to another. It would give better services to clients, would be much cheaper and more efficient in transferring information, and would eliminate a lot of paperwork.

The same interviewee felt that clients should not be asked their permission before inclusion in the integrated system, but stated that he, himself, would object to placement of his records on such a system.

Within the Ministry of Health, proposals are also being entertained to integrate the Senior Citizen's Drug benefit file with OHIP and other computerized information files held by that ministry. Such a system would be linked with several social service computer systems because case numbers and eligibility information of Family Benefits, Vocational Rehabilitation, General Welfare Assistance and several other social assistance recipients over 65 are already included in Drug Benefits files. The privacy of social assistance recipients under the age of 65 is also threatened by the possible integration of Ministry of Health systems. To check continued eligibility for health benefits, Family Benefits, General Welfare Assistance, Vocational Rehabilitation and other social assistance programs regularly submit computer tapes listing case numbers and eligibility information of recipients to OHIP. The majority of

interviewees in the Ministry of Community and Social Services were not aware of Ministry of Health proposals for integration or the implications of those proposals for the confidentiality of social service records.

D. Conclusions

1) The volume of personally identifiable records held by social service agencies and programs in Ontario is large and growing. The Ministry of Community and Social Services and its contracted agencies now hold the personal records of over 230,000 adults⁷⁹ and at least 300,000 children in the province. The one factor common to all these record subjects is possession of a problem for which society bears some responsibility. The definition of "problem" which justifies intervention by publicly-supported social services has grown considerably since the 1930's and continues to expand. With every expansion of definition, records systems about the private lives of Ontario residents have also expanded.

2) The types of information collected about those who come into contact with social service organizations are of the most personal and sensitive nature and often include subjective judgments. The social services

79 Ministry of Community and Social Services, 47th Annual Report for the Fiscal Year Ending March 31, 1978 (Toronto: September, 1978) 6. "In total, there were 232,850 beneficiaries [of allowances under the Family Benefits Act in the fiscal year]."

professions have traditionally valued information about the private lives of clients, in order to diagnose problems accurately, to define environmental influences and to design effective treatment plans. Furthermore, society has encouraged such practices by urging detailed investigations of social service applicants to protect public monies from fraudulent use, and to protect children from abuse and neglect. For example, under the provisions of the new Child Welfare Act, professional people will not only be under an obligation to report apparent child abuse observed in the course of their duties, but will be subject to a penalty for failing to report abuse. The resulting records often contain sensitive details about the physical and mental health, education, personal and family history, contacts with the criminal justice system, finances, sexual activities and living circumstances of applicants and clients.

3) Although a great deal of the personal information collected by social services is required by statute, many information elements collected are rationalized solely by history and administrative practice.

Several statutes give broad information collection powers to public social service agencies. For example, the statute requiring public assistance applicants who are deserted mothers of illegitimate children to prove their efforts to pursue paternal support for such children can only be enforced by requiring that applicants produce explicit identification and whereabouts of the father, which, in some cases, reveal details about the history of the relationship. Either of these requirements

may invade the privacy of applicants.⁸⁰ When formulated, the implications of social service legislation for the privacy of individuals have often been overlooked. However, many information elements in record systems held by social service agencies are unjustified by statute and are collected "because we have always done it that way." No assessment of the necessity of data items has ever been performed for any of the records systems investigated.

5) Methods and types of verification required for information supplied by subjects of personal social service records are often contentious.

Public assistance and day-care subsidy applicants must produce the most extensive forms of verification of all social service clients, including bank statements, insurance policies, birth certificates of all dependents, documentation of marriage and divorce, rent and utility receipts, letters from employers, school attendance records of all children over 16 years old and evidence of indebtedness. This verification can only be completed with the assistance of third parties, who become witnesses to the knowledge that a person is requesting public assistance, knowledge which may potentially be used against the applicant. From the client's viewpoint, an even more contentious

80 Form 80-00-107, Desertion Report, is utilized to obtain a detailed "Description and Information of Missing Person" (father), including eye colour, occupation, place of birth, height, weight, Social Insurance Number, OHIP number, visible identification features, employer's name and address, and addresses and phone numbers of relatives and associates. The form also provides a large area for "comments," and the note "If applicant/recipient does not know this information (missing person's date of birth, social insurance number, etc.), it is usually obtainable from documents in woman's possession."

practice is the occasional use of neighbours, acquaintances and housing inspections to verify personal information. The role of verification methods in the prevention of welfare cheating has not been proven.

6) Record storage practices inadequately and inconsistently safeguard personal information kept by the social services. In the absence of uniform policy governing this topic, different programs, agencies and personalities have developed their own divergent practices. The impact of varying security practices on the privacy of social service clients can only be negative. Cases of lost, misplaced and misappropriated records have already been reported and are likely to increase as volume of records increases.

7) Personal information contained in social service records is regularly exchanged among Ministry-funded programs, among several Ontario ministries, with local and federal government agencies and with various private interests, often without the client's informed, voluntary consent. Although many formal record transfer arrangements which require written client authorization do exist, especially in medical settings, most information is transferred informally without client knowledge. In their support for continuing frequent, unencumbered exchanges, adult services management appears to differ from Children's Services Division management, which supports closer monitoring of and written client permission for such exchanges, except in emergencies.

The primary effect on privacy of transfers unauthorized by the client is the loss of record subject control over uses and further dissemination of personal information. The potential for harm is enhanced when the record subject does not know what is contained in records transferred, whether or not s/he has given permission for the transfer. When a public assistance applicant, for example, signs a letter requesting a doctor to send a medical judgment about his/her functional condition to the Provincial Benefits Branch, in most cases the applicant does not see the contents of that judgment, which will be used to make far-reaching eligibility decisions about him/her. In these circumstances, the individual's permission for transfer arguably does not constitute informed consent, perhaps in contradiction to the intent of regulations governing transfer of medical information under The Health Disciplines Act.⁸¹ Because Ministry-held medical files are completely inaccessible to applicants and clients, no opportunity to challenge or update information after transfer can occur.

8) Access to personal social service records for research purposes is strictly controlled to protect client privacy. Despite a lack of ministry-wide policy governing research access to personal records, most programs and agencies investigated have initiated careful research procedures to avoid undue intrusion into client lives. The majority of

81 The Health Disciplines Act, R.R.O. 1974, 577/75, s. 26(21) states that, "giving information concerning a patient's condition or any professional services performed for a patient to any person other than the patient without the consent of the patient unless required to do so by law, constitutes professional misconduct on the part of a physician."

outside research proposals must be approved by a research committee or program director. To obtain approval, the proposals must contain provisions that guarantee the confidentiality and anonymity of subjects and their records, are potentially beneficial to the client population, and ensure voluntary subject consent for participation. No instances were reported of further dissemination of confidential information by research personnel, who must usually follow strict research guidelines of their host institutions, in addition to any requirements of the Ministry.

9) With the exception of some clients in Children's Services Division programs, subjects of social service records are denied access to their own files. Although the Ministry has not developed policy in this area, negative management attitudes and ad hoc practices have generally denied record subjects the opportunity to view their records. Supporters of subject access, primarily Children's Services management and a few of its agency directors, and the more numerous opponents of subject access among adult services management, field workers, records supervisors and clinicians, have presented the following arguments:

a) Exposure to sensitive items in records may negatively affect record subjects. Opponents predict harmful effects, subject shock and inability to handle certain types of information, such as diagnosis of a terminal illness or acute psychiatric disorder. Supporters of subject access point to studies indicating that lack of knowledge contributes to paranoia, concluding that a client will only benefit from openness which will assist in understanding and dealing with a condition.

b) Because most clients have never indicated an interest in reviewing their files, opponents predict that an open file policy would be utilized by only a few but would arouse suspicion and demands on the part of a previously uninterested population. Supporters of an open file policy feel that openness would arouse needed client interest in decision-making and would decrease client suspicion of the social service bureaucracy.

c) Because of the subjective nature of social service record-keeping, opponents of subject access predict client disagreement with many judgments in their files, resulting in costly time spent in recording challenges and perhaps court defence of recording agencies and personnel. Supporters of subject access counter that opening files will induce field workers, clinicians and other professionals to cease recording subjective comments and innuendo unconfirmed by evidence and to adopt more accurate, objective record-keeping practices.

d) Information contained in the file may have been given by third parties who were guaranteed confidentiality. Opponents of subject access feel that client knowledge of the identities of third parties would endanger their reputation, physical safety, or relationships with future clients, resulting in a hesitancy of information sources to cooperate with social service agencies. Supporters of subject access feel that the prospect of open files might end social service reliance on such biased third party sources as neighbours, while increasing the accountability of other sources to the client. Supporters also predict

that information sources will continue to cooperate with social service agencies if a policy allowing subject access is clarified when information is initially gathered.

The experiences of Ontario children's programs which have encouraged subject access, and of several states⁸² which have opened social service files to record subjects tend to support the contentions of those favouring subject access to files.

10) Although most social service record systems are now at least partially computerized, the introduction of automation has not decreased the volume of manual record files. All computerized systems investigated completely overlap manual systems. While public attention has focused on security of proliferating computer systems, the most obvious gaps in existing manual systems, which contain much more detailed and sensitive information, have been overlooked.

11) A large number of subjective data items and personal identifiers, including the Social Insurance Number, are transferred from manual records to computer systems, usually without the record subject's knowledge or permission. The dangers of computerizing subjective information include a loss of accountability to the subject, the

82 See Appendix to this chapter, Subject Access to Personal Records: Experiences in the Social Services. California, Connecticut, Massachusetts, Minnesota, Ohio, Utah and Virginia are among states which have opened social services files to subjects.

possibility of incompleteness or distortion, and the encouragement of permanent labelling, all of which jeopardize client privacy. The growing use of standard identifiers in social service data banks, especially the Social Insurance Number, also threatens client privacy. Theoretically, identifying numbers may be utilized to link information among many systems, enabling information seekers to "profile" record subjects and to create new variables describing the lifestyles and habits of record subjects.

12) During all phases of data preparation, computerization and print-out dissemination, personally identifiable records are inconsistently and in some cases inadequately protected against breaches of confidentiality. The lack of uniform record automation standards and policies and the presence of unsophisticated systems which depend on paper and telephone exchanges, have contributed to the current large volume of manual form transactions during computerization, and to varying security practices. Those seeking personal information are likely to take advantage of such inconsistencies, utilizing the weak links in systems to obtain unauthorized access to computer information.

13) A trend toward integration of social service computer systems, both within Ministry-held systems and between systems held by more than one ministry, may threaten the privacy of social service clients.

Integration among similar-function programs, such as different income maintenance programs, may actually ensure client privacy by eliminating record-keeping duplication. However, proposals for the integration of

public assistance data banks with those of housing programs, Ministry of Health systems, programs for the disabled, and day-care information systems have recently been entertained. The integration of different-function systems encourages the formation of extremely biased judgments about social service applicants and clients based on historical performance. This type of integration also decreases client control over the use and dissemination of personal information.

E. Alternatives

The implications of not according full privacy protection to social service client records are far-reaching. One consequence of inertia in addressing social service record-keeping issues is the possible growth in unauthorized dissemination, loss, theft, and illegal use of personal information. Considering the volume and the sensitivity of information gathered, the inconsistent controls on its storage and transfer, and the longevity of unused records, the number of cases of information loss, misuse, and misappropriation reported to the Commission is surprisingly low. The federal report Computers and Privacy noted the potential for increasing abuse of computerized information banks by business, financial, and criminal interests in 1972.⁸³ At that time,

83 Department of Communications and Department of Justice, Task Force on Computers and Privacy, Computers and Privacy (Ottawa: Queen's Printer, 1972), especially Chapter 8, "The Technological Prospects" and Chapter 9, "Security in Computerized Databanks."

most known abuses took place in the private sector. However, there is no reason to believe that the same interests would refrain from abusing government-held manual or computerized social service files, which could in some cases be more easily obtained and utilized for theft, blackmail, insurance investigations, security checks and public exposure of clients, former clients and their families. These types of unintended information uses could be embarrassing to the Ministry of Community and Social Services. More importantly, they could endanger the reputation, safety and livelihood of thousands of people.

A second consequence of continuing privacy-abusive record-keeping practices is mounting costs. Every question a field worker asks a client, all time spent investigating and verifying data sources, every person hired to record, compile, edit, update, store, program and transfer information, every cubic inch utilized to keep records in safes, filing cabinets, boxes and computers, costs taxpayers money. The total spent on personal information collection, storage, manipulation and computerization by the Ministry of Community and Social Services and its contracted agencies has not been assessed.

A third consequence of maintaining social service record-keeping in its present state is public criticism. More and more Ontario residents are becoming wary of information systems and computers. At the same time, a larger number of residents are utilizing government-funded social services. As the potential for greater involvement with the social services by middle-class, educated people increases, citizen toleration

for privacy abuses can be expected to decrease. Recent media reports of Social Insurance Number collection⁸⁴ illustrate the rising visibility of these issues.

Perhaps the most serious consequence of not reforming social service record-keeping is the damage to social service clients themselves. Handler and Hollingsworth concluded that the privacy-reducing attributes of our modern welfare system tend to stigmatize welfare clients:

Disclosing assets and resources, revealing the names of one's friends and associates, submitting to investigations and questioning, accounting for expenditures and social behaviour -- these are the price of receiving welfare. Loss of privacy is loss of dignity and is part of the shame of being a welfare recipient.

85

If the privacy of record subjects is to be protected, the aforementioned conclusions indicate a need for large-scale changes in social service record-keeping. Accordingly, alternative suggestions are presented to accomplish several objectives.

84 "Even babies get SIN as a clever idea grows and grows," Globe and Mail, September 19, 1978; "How the Mounties got a direct line to your SIN file," Globe and Mail, September 20, 1978; and "SIN misuse to be put before Parliament," Globe and Mail, September 25, 1978.

85 J.F. Handler and E.J. Hollingsworth, Stigma, Privacy and Other Attitudes of Welfare Recipients, (1969) 22 Stanford Law Review 2.

1. To Decrease Volume and Types of Records Held

a) Revise legislation to be less invasive of the privacy of social assistance applicants and recipients. Without statutory changes, most other revisions in social service record-keeping will be ineffective. Many social assistance statutes, by including ambiguous, undefined phrases such as "living together as husband and wife," impose undue interpretive responsibilities upon administrators.⁸⁶ These ambiguities sometimes necessitate the collection of large amounts of extraordinarily sensitive data. Others, such as the statutory requirement that mothers make efforts to pursue support from the putative fathers of their illegitimate children, can only be enforced with privacy-invasive practices.⁸⁷ Presumably, social service statutes were not designed purposefully to deny social assistance applicants the rights of other citizens. However, the attention devoted to protection of the public purse may have been at the expense of privacy considerations.

An alternative to the present legislative approach is the review of all proposed social service statutes and regulations by an inter-ministry

86 See Fox, Larry, Freedom of Information and the Administrative Process (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 10, 1979), introductory chapter.

87 One possible solution to this problem is the adoption of a statute similar to California's, which places defined limits upon questioning welfare applicants about paternity of children. (See California Welfare and Institutions Code 10850, s. 11477, as noted in the Privacy Protection Study Commission's report, Personal Privacy in an Information Society, Appendix 1: Privacy Law in the States (Washington, D.C.: USGPO, July, 1977).)

privacy committee prior to the second reading. A more objective evaluation of the effects of legislation might be obtained from a committee composed partially of non-government employees. The committee's duties would include specifying potentially privacy-invasive sections of proposed legislation, as well as devising alternatives for re-drafting any offensive passages.

In the meantime, adult social services could adopt the approach of the Children's Services Division in this area. The Task Force on Legislative Amendments reviewed all legislation governing children's services, drafted revisions to update and coordinate functions, and presented the proposed changes to the legislature. In the process of its work, the committee recognized the importance of child and parental rights, including the right of privacy, which led to recommendations such as one stipulating that alleged child abusers be informed of and be able to refute their inclusion in a child abuse registry.⁸⁸ The statutes governing adult social services deserve equal attention.

b) Avoid duplication of services. One factor often overlooked in privacy protection is the number of people and programs to which the same applicant for social services must give personal information. Every time an applicant sits in a different office to relay sensitive

88 Children's Services Division, Consultation Paper on Legislative Amendments (Toronto: December, 1977) 38-40; Children's Services Legislation: Changes Resulting from Consultation (Toronto: June, 1978) 15; Children's Services Legislation Summary (Toronto: June, 1978) 18.

information to another government agency, his/her private domain diminishes. This factor is especially important when assistance programs significantly overlap. For example, the overlap of Family Benefits and General Welfare Assistance clients is estimated (by interviewees) at 40 to 60%. Combining same-function programs will decrease the number of people handling personal information and the number of forms containing personal information circulating among various offices.⁸⁹

However, over-integration of unconnected services also endangers client privacy. The combination of income maintenance programs with programs for the disabled or retarded, for example, may not be advisable for this reason. If client privacy is to be respected, a person moving from one type of service to another must be afforded the anonymity to escape harmful labels and to "make a fresh start."

c) Limit the collection of subjective, undocumented data and judgments. By eliminating the "narrative" and "comments" sections of record forms, the social services would restore the privacy of many

89 An experiment combining the intake procedures for Family Benefits and General Welfare Assistance is already underway in three pilot locations of the province. Municipal field workers in Waterloo-Kitchener, for example, obtain information for Family Benefits applications during interviews of GWA applicants. The information is relayed by the municipal office to the provincial regional office of the Ministry of Community and Social Services. The experiment has not only eliminated dual information collection from clients of both programs, but has also significantly improved service delivery time. However, the program ended in June, 1979.

of its clients. Unless an item can be objectively and reliably documented, it probably should not be recorded. The utilization of neighbours and relatives as sources increases the likelihood of subjectivity of information, and should also be avoided.⁹⁰ As more social service cases come before appeal boards and courts, objectivity will become even more important. No court is likely to accept a judgment that an applicant is "unmotivated," for example, without adequate evidence. Opponents of this viewpoint see increasing objectivity in social services decision-making as decreasing the opportunities for compassion and flexibility in unusual circumstances. While this argument may have merits, its detractors point out that objectivity also decreases the opportunities for uneven administrative decisions biased against clients in various kinds of circumstances.

d) Regularly review the information components of all records systems, including the justification for collection of every data item. The rationale that "we have always done it that way," or that "we might use it someday," or that "the computer needs it," are not adequate reasons to ask social service clients probing questions about their present and

90 Regarding this subject, the U.S. National Assembly for Social Policy and Development, in A New Look at Confidentiality in Social Welfare Services (New York: 1973), has commented,

The client should be the primary source of information about himself and his problems ... Safeguards should be set by the agency for seeking, accepting and recording information from other sources. If there is information the client cannot provide, or if verification is required, he and the worker should decide together what other sources are to be used and the method for obtaining the needed detail.

past lives. If an item is not necessary for decision-making, it should not be included. Where disagreements about the usefulness of a particular data item occur, program managers might request the opinion of a privacy committee.

e) Destroy or de-identify the personal records of unaccepted applicants, terminated clients and juveniles reaching the age of majority. According to the cumulative estimates of interviewees, the regular destruction of inactive and outdated records would reduce the present volume of personal social service records in Ontario by over 150,000 individual files. With only active and pertinent records stored, the data security responsibilities of the Ministry would become more manageable.⁹¹ The continuing storage of records of terminated juvenile clients and of those transferred to adult services at the age of 18 is especially dangerous, encouraging the unauthorized dissemination of possibly detrimental information about juveniles to the public and to adult authorities. The American Juvenile Justice Standards Project has concluded that the intent of special juvenile laws and special juvenile programs to protect children from the adult world can only be upheld if juvenile records are strictly separated from adult records, and if those records are destroyed when record subjects reach the age of

91 The U.S. National Assembly for Social Policy and Development, op.cit., recommends that

Each agency should have a policy regarding what records are to be retained, what kept for archives, and over how long a period of time ... it is probably that most such records could be destroyed in a given time after the case is closed or discontinued.

majority.⁹² This conclusion appears to be equally applicable to Canadian juvenile programs.

The wholesale destruction of personal records may pose problems for those engaged in valuable social research, program planning and evaluation of services. One option in addressing the problem is the removal from inactive files of all personal identifiers, such as name, address, Social Insurance Number, file number, OHIP number and place of origin. If this option were chosen, record-keepers would have to exercise care in removing all identifying information of all subjects named in each record -- a considerable task for social service agencies keeping family case files.

2. To Revise Record-Keeping Policies and Practices

a) Utilize the resources and expertise of the Ministry's committees to develop consistent policy addressing privacy and confidentiality issues. The Children's Services Case Information Disclosure Task Force, Standards Development Advisory Committee, Children's Rights Working Group and the ministry-wide Committee on Confidentiality have amassed

92 See Institute of Judicial Administration, American Bar Association, Juvenile Justice Standards Project, Standards Relating to Juvenile Records and Information Systems (Cambridge, Mass.: Ballinger, 1977). Practical suggestions for implementing regulations regarding juvenile records may be found in Zimmerman, King and O'Neill, How to Implement Privacy and Security (Washington, D.C.: Theorem Corporation, 1976).

a large number of materials examining these issues. Members of these groups have devoted considerable time in reviewing program practices, writing working papers, assessing the viewpoints of field personnel and formulating standards and guidelines to protect the privacy and confidentiality of social service clients and records. The recommendations of Children's Services committees have already been utilized by Division management in policy development. By consistently utilizing the output of the many committees investigating problems in the area, senior management in all divisions and programs could quickly and decisively close an important policy gap.⁹³

b) Formulate standards and guidelines governing personal record-keeping. Other than a working paper on the subject prepared by two members of the Children's Services Case Information Disclosure Task Force, no standards and guidelines for personal record-keeping have been developed by the Ministry of Community and Social Services. Without direction, inconsistent and sometimes careless record-keeping practices, varying by program, agency, location and personality have been propagated. A thoughtfully conceived, forthright and comprehensive group of statements, modelled on work by the New South Wales Privacy

93 The U.S. National Assembly for Social Policy and Development, op. cit., concludes,

Every agency should define its policy on confidentiality and state how it will be implemented ... workers, as agency representatives, must inevitably assume responsibility for some individual decisions and interpretations of policy. These will be made more soundly if against the background of well-stated agency policy.

Committee,⁹⁴ might provoke much-needed attention to privacy and confidentiality of social service client records. These standards and guidelines would apply to the following problem areas:

- . Collection of information
- . Verification and updating of information
- . Record storage
- . Record destruction
- . Transfer of personal information
- . Research access
- . Computerization of personal records

c) Define and institute subject record rights. Perhaps the most distressing discovery of this investigation was the almost total absence of subject rights regarding personal records. Even statutes and regulations, designed to promote applicant and client rights of review of evidence for appeal purposes, have sometimes been abused. Except in certain Children's Services programs, clients have been prohibited from taking part in decision-making about their records. A desirable alternative to this situation would be the inclusion of record subject rights throughout government-sponsored social service programs. At a minimum, these would include:

- 1) The right of refusal to relate private, sensitive information. Statements defining this right would carefully outline and specify

94 See New South Wales Privacy Committee, Guidelines for the Operation of Personal Data Systems, (Exposure Draft), op.cit.

information required for service, possible consequences of refusal to give required information, and optional information.

2) The right of physical privacy. This right would prohibit housing inspections for the purpose of information collection, especially of bedrooms and private belongings. All applicants and clients would have the right to be personally interviewed in a private, quiet office.

3) The right of access to records. It would be difficult at best for a subject to protect his interests, correct mistakes, participate in decision-making or control use of records if s/he did not know exactly what was contained in his/her file. This right would make available any information in any personal record, including field notes, to the record subject. The dire predictions of those who object to this right appear to have little basis in reality, according to the experience of several jurisdictions which have made all types of sensitive personal files available to subjects.⁹⁵

Implementing this right might be far easier than many interviewees supposed. The mechanisms, procedures, and physical space for subject access already exist in many Ministry programs. For example, Provincial

95 U.S. federal law requires that all states allow subject access to federally funded welfare program files. Additionally, nine states, Arkansas, California, Connecticut, Indiana, Massachusetts, Minnesota, Ohio, Utah, and Virginia, have implemented privacy legislation which allows subject access to the subjects' government-held data files. (See Privacy Law in the States, op.cit.). A survey of welfare administrators in those states is contained in the Appendix.

Benefits records are now available to requesting employees through the mails or in person, and could be extended to requesting subjects with only minor changes in policy. If the Canadian case is similar to the American, the actual number of subjects accessing their files will not require any additional bureaucratic machinery. Moreover, the suspicions of third party information sources about repercussions of subject access could be allayed by informing them of the policy change at the time of information collection. A simple statement could be added to medical assessment and other forms, noting that the contents of the form would be open for inspection by record subjects, and that objections to subject review should be directed to a privacy committee or management level staff member. The Ministry might mediate those cases in which information sources disagreed with subject access for protective or other reasons, by giving access to documents in contention to a third party nominated by the subject.⁹⁶

Interviewees at all levels foresaw the strongest objections to subject access from the medical profession. The present policy of maintaining separate medical files, unavailable to social service clients under any circumstances including Board of Review hearings, while other material may occasionally be perused, has no basis in statute or privilege. The policy apparently arose from clinician pressure and administrative tradition. The denial of subject access to medical records may be

96 This approach has been endorsed by Fair Information Practices Acts in Ohio (1976) and California (1977), and by the Australian Freedom of Information Bill (1978, Part III, s. 30(3)).

contrary to the spirit of The Health Disciplines Act, 1974, which prohibits transfer of medical records without patient consent.⁹⁷

Voluntary, informed consent implies subject knowledge of the contents of records which doctors transfer to social service agencies. If the medical profession encouraged subject access and voluntary, informed consent before record contents were released to other agencies, subject access to medical information would no longer be an issue for the social services.⁹⁸

4) The right of awareness of personal data security practices. If social service clients were aware of inconsistent and in some cases, inadequate protection of extremely sensitive data about themselves, they might refuse to answer many questions typically asked by social service personnel. Conversely, if data security were tightened, client knowledge of security precautions could strengthen confidence in the social service bureaucracy and encourage openness. In either case, subject awareness of data protection practices might induce all

97 The Health Disciplines Act, R.R.O. 1974, 577/75, s. 26(21), states that giving information concerning a patient's condition or any professional services performed for a patient to any person other than the patient without the consent of the patient unless required to do so by law, constitutes professional misconduct on the part of a physician.

98 The Ontario Medical Association, in a brief presented to the Commission on Freedom of Information and Individual Privacy, October 11, 1977, advocated only limited access to medical records by subjects. It stated that, "patients who are unaware of the content of their records and unsure of their ability psychologically to handle the information need the protection of the professionals who produce the records and can assess the hazards to the best interests of the patient in providing access."

information sources, recipients and systems managers to handle personal records in a responsible, consistent fashion.

In a related matter, the extraordinary security precautions for medical data, at the expense of equal precautions for other sensitive data, are potentially harmful to subject privacy. A sensible solution to this inconsistency would be furthered if equally stringent rules were applied to the protection of all data which clients might regard as sensitive.

5) The right of disagreement. Subjects reviewing their records would occasionally wish to correct and update them. This right would ensure the prompt correction of acknowledged mistakes in files, and ensure the recording of any client disagreements in judgment with social recording personnel, without repercussions to the record subject.

6) The right of control over information transfers. This right could be given to subjects only if social service personnel were willing to limit informal information exchanges and to obtain voluntary signed client authorization for all information transfers, except in emergencies or cases brought to the police or courts for action.⁹⁹ Instituting

99 The U.S. National Assembly for Social Policy and Development, op. cit., views client consent for all transfers as one of the most important tenets of privacy protection.

Information about an individual client may not be shared with any other individual or agency without his express consent ... Blanket consent, real, implied or assumed, is never acceptable for either gathering or giving information, whether factual or evaluative ...

the right of control entails more than requiring specific client permission for release of any data from social service files and from other parties; it means keeping logs in every client folder to record transactions, and notifying subjects of those transactions. The latter function could be accomplished by regularly mailing subjects lists of all people accessing their files, or much less expensively by producing logs upon subject request.

Because the prospect of limiting information transfers was contentious to many management level interviewees, the establishment of a client right controlling information exchanges would likely encounter opposition. Those predicting abuse of such a right might be reassured by the experience of both the Ontario Ministry of Correctional Services and American federally-sponsored criminal justice programs,¹⁰⁰ which standardly provide subject authorization of information exchanges.

d) Educate and train all social services employees to be aware of and to respect the privacy of applicants and clients and to safeguard the confidentiality of personal records. One deterrent to the revision of record-keeping policies and practices has been lack of knowledge about privacy issues. For many of those interviewed, our research questions provided an opportunity not given before to think about and to discuss record-keeping's relationship to privacy. Most interviewees had been given no instruction in the data protection responsibilities

100 Institute of Judicial Administration, American Bar Association, op.cit.

of social service record-keeping during formal training. Training personnel for several social service programs acknowledged the absence of direction in this area.

One rationale given for the inattention to privacy and confidentiality issues during training has been the assumption that colleges, universities, and professional societies educate their pupils and members in such subjects. In fact, the curricula of Ontario schools of social work, computer science faculties, graduate programs in psychology, medicine, and public administration rarely include required courses in professional ethics or references to the effects of social service record-keeping. John Carroll has noted some of the grave implications of apathy about these issues in a survey of the ethics of computer science students.¹⁰¹

Professional organizations could play a significant role in the development of record-keeping standards and the training of members in proper record-keeping skills. Some professional organizations, such as the Canadian Association of Social Workers, have provoked discussions about the problems of privacy protection and record-keeping in

101 Carroll, John, Lecture at University of Western Ontario, October 10, 1978, quoted in "Universities teach illegal computer use, professor says," Globe and Mail, October 11, 1978. Professor Carroll's ideas for improving computer scientist education and ethics are also expounded in two articles, "How to Tell an Honest Programmer," and "The Case for Computer Scientists Teaching Computer Science or Digit-Alice in Squanderland" and the monograph, Prevention of Computer-Based Fraud (London, Ont.: University of Western Ontario, September 30, 1978).

conference workshops. However, the Association and other voluntary associations could hold training sessions specifically to address these issues, and could define precise professional obligations regarding privacy.¹⁰² Those practicing unprofessional conduct could be sanctioned by their peers, in the same manner that medical practitioners are now sanctioned for disregarding client privacy.

The alternative to dependence upon the formal schooling or professional memberships of incoming employees, is comprehensive training in the subjects of privacy and personal record-keeping for all personnel of the Ministry of Community and Social Services and its contracted agencies. The type of training envisioned would encompass discussion of the issues, identification of privacy and confidentiality problems, presentation of various approaches to social service record-keeping, and development of skills in handling record-keeping situations with applicants and clients. Continuing emphasis on these areas over several years could significantly improve the policies and practices of those administering social services.

e) Enforce Statutes, Regulations, Standards and other policies governing privacy and personal record-keeping in the social services.
Without the means of enforcement, policies governing personal record-

102 The present code of ethics of the Canadian Association of Professional Social Workers (approved by the Board of Directors of the Canadian Association of Social Workers, June 13, 1970) includes the obligations "to respect the privacy, dignity and other rights of persons," and "to use in a responsible manner information obtained in the course of professional relationships."

keeping will be weak and ineffective. One apparent reason for past inconsistencies in record-keeping and information transfer practices has been a distinct absence of penalties for violating client privacy or disregarding record confidentiality. Although many verbal reprimands have been issued when personal information has been revealed, written reprimands, loss of pay and dismissals have been rare, even for serious violations of confidentiality. Such light penalties may not discourage social services personnel who handle sensitive records from misusing or misappropriating personal information in ways extremely harmful to record subjects.

At least two options might improve the enforcement aspects of record-keeping policies. First, agreement to follow standards of record privacy and confidentiality could be specified as a condition of employment, a change already initiated in at least one Provincial Benefits district office and several agencies administering other social service programs. Every incoming employee would then be fully aware of his/her data protection responsibilities and of the penalties for abrogating those responsibilities. For example, Statistics Canada maintains stiff penalties for violating the confidentiality of record subjects.¹⁰³ This precedent might be followed in developing employment conditions in Ontario.

103 Statistics Act, R.S.C. 1970, c. 257, s. 34 states, "Every person employed in the execution of any duty under this Act or any regulation who, (a) after having taken the prescribed oath, deserts from his duty, or wilfully makes any false declaration, statement or return concerning any such matter; (b) in the pretended

Secondly, contracts between the Ministry of Community and Social Services and several hundred service agencies could require compliance with the record-keeping standards recommended in this report. Present contract provisions already give the Ministry the right to inspect records and record-keeping practices, and place the responsibility for compliance upon agency directors or personnel specified by directors.¹⁰⁴ Non-compliance with standards could result in suspension or loss of funding. If these options were followed, the need to resolve the question of record ownership would be diminished.

3. To Ensure Subject Privacy in Computerized Social Service Personal Record Systems:

a) Implement computerized record systems only after careful development and review of policies protecting record subject privacy. Uniform record automation standards could prevent needless automation of certain

103 (cont'd) performance of his duties thereunder, obtains or seeks to obtain information that is not duly authorized to obtain; or (c) fails to keep inviolate the secrecy of the information gathered or entered on the schedules and forms, and who, except as allowed by this Act and the regulations, divulges the contents of any schedule or form filled in, in pursuance of this Act or any regulation, or any information furnished in pursuance of this Act or any regulation; is guilty of an offence and is liable, on summary conviction, to a fine not exceeding three hundred dollars, or to imprisonment for a term not exceeding six months, or to both."

104 In purchase of service contracts with social service agencies, the Ministry generally includes a clause worded in the following manner:

The corporation will keep such books and records of account as may be required by Ontario with respect to the program and make any or all of such records and books of account available to Ontario upon request.

manual data, mishandling of computerized data, unauthorized transfers of such data and the formation of client dossiers from several related information banks. Such policies might also improve client confidence in automation. J.H. Noble, among many experts in the field, has suggested that

Social work and health professionals should be most circumspect in reviewing various proposals for computerizing portions of existing information systems because their interests in protecting confidentiality may be vitally affected. This matter goes beyond actualities to include images and impressions. Computerized information systems that do in fact safeguard confidentiality, but fail to give the impression of doing so, are a threat to the client-professional relationship because loss of faith could prevent people in need of help from requesting it.

105

b) Eliminate unnecessary overlap of manual and computerized record files and forms. Once files are computerized and retrievable by terminal, the utility of maintaining several duplicative manual files is questionable. To end this practice would help safeguard client privacy. Similarly, the elimination of many personally identifiable computer information forms, now stored in scattered insecure places, would decrease the potential for invasion of client privacy.

c) Discontinue the automation and computer storage of subjective data items and personal identifiers such as the Social Insurance Number. In the absence of adequate security measures and policies ensuring privacy, the presence of dossier-type information systems may

105 Noble, J.H., Protecting the Public's Privacy in Computerized Health and Welfare Information Systems, (1971) 16 Social Work 37.

significantly endanger client privacy. Further recommendations about these subjects may be found in Chapter IV and Chapter V of this report.

d) Disallow integration of computerized record systems among different-function programs. Until consistent security precautions and policies are implemented, personal data linkages of this type may also significantly endanger client privacy.

Noble and others concur with this viewpoint.

In view of the dossier-type systems's vulnerability to abuse, the anxiety of citizens about privacy and the computer age, and the sensitivity of the client-professional relationship to real or imagined breaches of confidence, the social work and health professions are justified in taking a conservative stance toward information systems containing identifying data on clients.

106

e) Observe the same subject rights in relationship to computerized personal record systems as suggested for all record systems. The implementation of such rights would mean client awareness of the automation of his/her record, the option to refuse to place information on the system, the opportunity to review and challenge the veracity of personal computerized records, and awareness of and control over transfer of personal information among such systems.

APPENDIX VIII.A

SUBJECT ACCESS TO PERSONAL RECORDS

Experiences in the Social Services

The issue of subject access to personal records has provoked a great deal of controversy among administrators of Ontario social service programs. The concerns about such a provision, contained in either a privacy or a freedom of information statute, are based primarily upon two characteristics of social service record keeping: many personal files contain subjective, opinionated data; and third party sources, such as doctors, psychologists, family members and neighbours often contribute information to personal files on the assumption of confidentiality. Because of such characteristics, some administrators predict that universal subject access may have the following negative effects upon social service record-keeping:

- 1) Subject access will be excessively costly and time consuming, necessitating the establishment of new bureaucratic units simply to process the expected large number of access requests and to review files before subject viewing.
- 2) It will inhibit information collection. Third party sources will be more reluctant to give information about social service clients, especially information critical of the client. For example, neighbours

and others who have traditionally felt free to complain about welfare recipients surreptitiously taking employment or about parents abusing their children, will no longer be willing to report their opinions, fearing retribution by record subjects who read their files. In a similar vein, doctors and other professionals, who now feel free to give assessments of clients to social service agencies, will refuse to perform such assessments if clients may see the results, fearing possible civil suits.

3) Subject access will change information storage practices, inducing workers to keep "double files," i.e. one official file containing fairly innocuous information which the client sees upon request, and another "desk drawer" or "note-pad" file, containing more sensitive and subjective data of which the client is unaware.

4) The reactions of record subjects who view their records may be damaging to both the mental health of those subjects and the physical safety of record-keepers. For example, a mentally unstable record subject may be unable to cope with information about his/her illness, and may suffer a breakdown, or may physically attack the source of that information.

To assess the accuracy of these predictions, we conducted a survey in the fall of 1978 of social service administrators in eight states and

one province which authorize subject access.¹⁰⁷ Their evaluations of the impact of subject access were requested in questionnaires administered by mail or telephone. A copy of the instrument, which contains seven open-ended questions, and a list of respondents are appended to this document.

It should be noted that the mechanisms which provide subject access to records, as well as the length of time they have been operating, vary among the nine jurisdictions investigated. Seven of the states have enacted privacy legislation which includes subject access stipulations:

- 1) California: Fair Information Practices Act (1977)
- 2) Connecticut: Personal Data Act (1977)
- 3) Massachusetts: Fair Information Practices Act (1976, 1977)
- 4) Minnesota: Data Security and Privacy Act (1974, 1975)
- 5) Ohio: Personal Information Control Act (1976)
- 6) Utah: Information Practices Act (1975)
- 7) Virginia: Privacy Protection Act (1976)¹⁰⁸

107 California, Connecticut, Delaware, Massachusetts, Minnesota, Ohio, Utah, Virginia and Nova Scotia. Colorado, New York and Oregon also received survey instruments but did not reply. Arkansas, which enacted a privacy statute in 1975, replied that the state was unable to evaluate the impact of subject access in any area because the overseeing body for the Act was not funded by the legislature.

108 Smith, Robert Ellis and Snyder, Keith D., Compilation of State and Federal Privacy Laws (Washington, D.C.: Privacy Journal, 1978) 86-129; and correspondence from the California Department of Social Services, September 7, 1978.

Typical wording dealing with subject access is contained in the Connecticut Personal Data Act: (s. 4(d)) Each agency shall make available to a person, upon request, the record kept under

(cont'd)

One of the states surveyed, Delaware, has opened up social service records to clients as a result of federal regulations, which require that state programs receiving federal funds conform to subject access provisions of the American Privacy Act of 1974.¹⁰⁹ Nova Scotia has not enacted privacy legislation, but provides for subject access to records under its Freedom of Information Act of 1977.

The scope of each of the subject access provisions also varies substantially from jurisdictions to jurisdiction. Some state laws apply to county and municipal social service agencies; others apply only to state level agencies. In this regard, Massachusetts', Minnesota's and Virginia's statutes are the most far-reaching, requiring municipal and even some quasi-public and private entities to provide subject access to records, while California's, Connecticut's and Utah's are restricted to only state-administered agencies. The Ohio statute falls between

108 (cont'd) subsection (c) of this section; (s. 4(g)) ... disclose to a person, upon request, all personal data concerning him which is maintained by the agency. If disclosure of personal data is made under this subsection, the agency shall not disclose any personal data concerning persons other than the requesting person; (s. 4(h)) Establish procedures which: (1) Allow a person to contest the accuracy, completeness or relevancy of his personal data; (2) Allow personal data to be corrected upon request of a person when the agency concurs in the proposed correction; (3) Allow a person who believes that the agency maintains inaccurate or incomplete personal data concerning him to add a statement to the record setting forth what he believes to be an accurate or complete version of that personal data. Such a statement shall become a permanent part of the agency's personal data system, and shall be disclosed to any individual, agency or organization to which the disputed personal data is disclosed.

109 U.S. Federal Regulation Number 45 CFR 205.50.

the two extremes, applying to state and locally-administered government agencies, but not to private corporations.

The ability to access medical information, which is often considered the most sensitive data in personal social service files, also varies among those surveyed. That right is officially granted only by Minnesota (under a 1975 amendment to its Privacy Act). Other states either specifically or generally exempt medical records (California,¹¹⁰ Connecticut,¹¹¹ Ohio,¹¹²) from subject access, although both California's and Ohio's Acts allow the release of medical, psychiatric or psychological information "to the person's personal physician, psychiatrist or psychologist, or to an attorney who presents a signed written authorization made by the person"¹¹³ Information statutes passed in Massachusetts, Nova Scotia, Utah and Virginia do not address the issue.

110 s. 1798.3(3).

111 s. 5.

112 s. 1347.04(B).

113 Ohio s. 1347.08(C).

Survey Results

1. Number of Access Requests

All the social service administrators surveyed report a surprisingly low number of subject access requests, even where the new stipulation has been well-publicized and where social service clients have been encouraged to exercise their new rights.

For example, Minnesota's largest urban country, which provides social services for approximately 33,000 people, counted only 55 requests in its first year of privacy law implementation, "after a fairly extensive effort to let applicants and recipients know that they were entitled to access their records."¹¹⁴ According to one interviewee in Minnesota, applications for record reviews have only slightly increased since 1975 because of Legal Aid Society activity on the behalf of welfare clients. Other jurisdictions surveyed have not recorded exact numbers of requests received, but report that the low volume (two to twenty per year) has been easily handled by local social service offices without

114 Hennepin County (Minnesota) Welfare Department, testimony given by Dennis E. Maher to the U.S. Privacy Protection Study Commission, January 11, 1977. Hennepin County prints the following message on forms received by social service applicants and clients: You may request in writing to be shown information about yourself that is maintained by our department. There is no cost for this service, but there is a small copy charge should you need copies.

setting up any additional bureaucratic machinery and without devoting extra staff time to file reviews.

When asked to comment upon this phenomenon, welfare administrators speculated that the statutorily guaranteed opportunity to examine one's file might serve the same purpose as actually reviewing that file. Social service clients who have been suspicious of record-keepers may feel that access provisions serve as detriments to the placement of subjective judgements and undocumented data in personal files. In fact, all of those administrators surveyed stated that access provisions had had this positive effect upon social service record-keeping.

Many jurisdictions have found that certain groups of social service record subjects are more likely to request record access than others. Nova Scotia, for example, has encountered more requests from former Family Benefits recipients, adoptees desiring identity information, social service personnel, Old Age Pension applicants, and contracted agency directors wishing to see inspection reports than from other client groups.

An unforeseen problem in implementing subject access -- abuse of the law by individual "cranks" -- has been experienced by at least one jurisdiction surveyed. One person, "who has nothing to do but write letters, has caused the California Department of Social Services and many 'watchdog' agencies to spend hundreds of hours answering fictitious

charges."¹¹⁵ This problem may be a result of omissions in the law itself. Abuse by "cranks" is prevented in other jurisdictions by granting the right of access to an individual record subject only once per year (Ohio) or once every six months (Minnesota).

2. Effect upon Information Collection and Transfer

Two questions were considered appropriate to address this topic. First, what has been the effect of subject access upon professional third party contributions to personal records? Respondents unanimously replied that subject access has had only a negligible impact upon the professional exchange of record subject information. A Virginia administrator typically observed that:

Some professionals have always refused to participate in this department's work. They still have the option to refuse to give an assessment, but the ones who always cooperated have not been affected by the law and still provide us with their objective opinions.

116

Hennepin County, Minnesota, testimony also supports the view that professionals have not been inhibited from expressing negative opinions when necessary:

115 Correspondence from James D. Simon, Attorney for the California Department of Social Services, dated September 7, 1978.

116 Steven Lewis, Communications Director for Virginia Welfare Department, in interview, November 14, 1978.

We have no documentation that access has created a reluctance to record information to the detriment of the client served. 117

Administrators in California, Connecticut, Minnesota and Ohio pointed out that under their privacy statutes, client permission must be obtained before a third party opinion is solicited, meaning that the client in most cases knows the professional and the nature of his/her judgment before that judgment becomes part of the client's social service agency record. Minnesota and Utah social service agencies, among others, have been able to induce the cooperation of third party professionals in implementing the law through extensive training and education.

However, the lack of problems experienced by Utah may be partly attributable to administrative guidelines which (in apparent contradiction to the spirit of the Utah law) deny subject access to psychiatric or other medical reports without the permission of the contributing doctor. This guideline has not been challenged in court.¹¹⁸

117 Hennepin County (Minnesota) Welfare Department, op.cit., 6.

118 According to one administrator in Nova Scotia, professional exchanges about clients may be much more constrained in Canada by the possibility of civil suits than by access legislation. The 1964 (A.C. 465) Hedley-Byrne case in England questioned the liability of a professional giving inaccurate advice about a client to an agency of a company attempting to assess the client's risk for business purposes. Arguments based on that case have been applied successfully in several Canadian suits, one of which involved a clerk in a Manitoba municipal welfare office. Thus far, neither welfare workers nor doctors have been sued in Canada merely for giving false information about a client to a third party, but the probability of such an action has certainly risen since Hedley-Byrne.

A second question addressing the issue of subject access upon third party contributions to records provoked more negative replies from survey respondents. Subject access may have a limiting effect upon non-professional third party contributions to personal records. California social service administrators, for example, believe that that state's new Information Practices Act may create difficulties for adoption investigations. Although the law permits the deletion of names of sources who were promised confidentiality from the record, "the content of statements will probably pinpoint the sources despite any disguises used," possibly influencing associates of prospective parents to be less than open with adoption authorities.¹¹⁹ Since the enactment of state privacy laws, both Minnesota and Virginia report decreased child abuse complaints, which have been attributed to the reluctance of third parties to become even anonymous contributors to a record which alleged child abusers may in some cases examine. Delaware and Massachusetts social service administrators also feel that subject access has inhibited neighbours and other private parties associated with social service clients from contributing information to authorities.

Four jurisdictions queried (Connecticut, Ohio, Nova Scotia and Utah) have not encountered any problems with third party cooperation. However, the former two statutorily limit subject access to many types of data, and the latter two have invoked administrative guidelines -- again, in

119 Correspondence from James D. Simon, op.cit.

apparent contradiction to the spirit of the law -- preventing subject access to some "potentially damaging information" on the record.¹²⁰ Thus far, such guidelines have not been challenged by record subjects or overseeing bodies in courts.

3. Effect Upon Information Storage Practices

Six of the nine social service administrations surveyed report no changes in filing practices resulting from subject access to records. However, respondents in three jurisdictions have noticed a tendency toward "double filing" to prevent subject access to "sensitive" records. Problems in Nova Scotia, Minnesota and Utah have revolved around the definition of "official file." Nova Scotia social service personnel, for example, have removed medical opinions and "damaging information" from client files, claiming that these are not part of the client's "official file," even though the law does not specifically exempt them from subject access. Minnesota authorities report that some social service records, including psychiatric assessments, are still designated "confidential," exempting them from subject access under the law, despite the intent of the law to reveal any information used for

120 In Nova Scotia, verbatim welfare worker notes and medical records are not released to record subjects, according to Mr. T. Daley, at the Ministry of Social Services. The Utah Division of Family Services Agency Standards on the Information Practices Act, also prohibits the release of third-party documents without a signed release from the third party (IIIE122), the release of records "damaging to the consumer," and some narrative records (IIIE125, 127).

decision-making purposes to record subjects. Utah social service personnel have followed departmental administrative guidelines which encourage the removal of welfare worker notes from the "official file" available to the record subject, and leave only a summary of the notes in the "official file." No social service clients in any of these three jurisdictions have challenged such definitions.

4. Reactions of Record Subjects

The observations of social service administrators indicate that predictions of violent subject reactions as a result of record access are greatly exaggerated. None of the nine jurisdictions surveyed has experienced physical assaults upon information sources or welfare workers by clients assessing their records. To the knowledge of those interviewed, clients have not suffered mental breakdowns or other damage after reviewing their records. A Minnesota policy analyst noted that long before the introduction of privacy legislation in that state, mental hospitals allowed patients to review their records in the presence of a patient advocate, with no reported detrimental effects. Connecticut, Massachusetts and Utah also granted hospital patients the right to see their records under statutes preceding privacy legislation.

Record subjects are only beginning to exercise legal rights of redress found in information statutes against social services record-keepers. According to the administrators surveyed, the increasing number of

appeals and court cases brought by social service clients is not a result of record subject rights legislation, but more likely the result of a general trend toward social service client advocacy. Respondents in two states, Delaware and Utah, each reported a civil suit resulting from damaging information contained in a social service record, but in both cases the information was transferred to a third party by a welfare worker without the client's permission. In the majority of jurisdictions that allow record subject access, administrators believe the threat of civil suits has encouraged social service personnel to be more objective in their record-keeping and to document their allegations more thoroughly.

Conclusions

In reference to the four predicted impacts of subject access to personal records kept by social service agencies, our survey research data led to the following conclusions:

- 1) Subject access to personal social service records will probably be neither excessively costly nor excessively time-consuming. The number of requests to review records is likely to be small enough for present bureaucratic units to handle without hiring extra personnel.
- 2) Subject access can be expected to slightly inhibit information collection from professional third parties, especially if medical

information is given directly to record subjects, rather than to an intermediary such as a subject's personal physician or attorney. At the same time, the prospect of subject access is likely to improve the quality of professional record-keeping, eliminating subjective, undocumented judgments. Perhaps the greatest impact of subject access is likely to be its negative influence upon the reporting of child abuse, foster parent or adoptive parent adequacy and welfare recipient fraud, by neighbours and others who may fear detection and retribution by record subjects, even if reporter identities are officially protected.

3) The impact of subject access upon information storage practice appears to depend upon the exactness of phraseology in information statutes. The definition of "official file" or "file" plays a particularly important role in affecting administrative adaptation to the law. "Double filing" appears unlikely to become a major problem.

4) No reports from any jurisdiction surveyed justify the conclusion that record subjects who review their records are likely to suffer mental breakdowns or to physically attack information sources such as welfare workers or neighbours. In fact, the evidence indicates that record reviews reassure social service clients, and help eliminate suspicions of record keepers and government.

CHAPTER IX

EDUCATION

A. Introduction

Until April, 1979, two ministries in the province of Ontario held records in relation to education: the Ministry of Education and the Ministry of Colleges and Universities. Now, the Ministry of Education encompasses the latter and the combined functions are examined in this chapter. The Ministry oversees public education for the province of Ontario through powers granted to it under the Education Act.¹ It coordinates the 194 boards of education around the province to ensure consistency of curriculum and administrative standards in elementary and secondary education, provided by both public and separate school boards, and through accredited private schools. Curriculum and course standards are set by the ministry, but the local boards wield a great deal of independent power for it is they who hire and fire teachers and administrators and who keep most records on both students and teachers. It is on these two groups of individuals that we have concentrated our examination of personal record-keeping in elementary

1 Education Act, 1974, S.O. 1974, c. 109.

and secondary education. In gathering data for this study we spoke with ministry officials, administrators at boards of education, teachers, and representatives of professional organizations. At the colleges and universities level, we examined record systems maintained formerly by the Ministry of Colleges and Universities, and particularly the student awards program. In addition, we looked at records kept by the ministry on people involved in the Industrial Training Program and in trade certification.

We will deal first with student records and then with teacher records. Following this we will describe the records kept by the province in relation to post-secondary education.

B. Student Records

Student Records are defined by the Education Act, 1974 and its regulations in terms of certain forms maintained by the principal of the school. There is also a ministry-held record on computer tape, indicating the final grade thirteen marks achieved by individual students. The Ministry of Health is responsible for a third set of personal records about students, kept by public health nurses in the schools. Two relatively minor systems of personal records maintained by the Ministry of Education are the "Correspondence Education Branch" records and the "Integrated School System" files.

A brief description will suffice for these latter two systems. The Correspondence Education Branch keeps transcripts, application forms and statements of completion for 250,000 correspondence students. These are maintained as a paper file, and are retained for three years after the student separates from the program. Most correspondence students are adults.

The Integrated School System is available to high schools on an optional basis to record information about students by means of computer. Biographical information, timetables and course marks may be recorded in this way. Approximately 150 high schools use the facility. The Education Data Processing Branch employees and user schools are the only ones with access to it. It is possible that such a data base will be extended to include information from all schools. At present it is neither an official nor mandatory system, but merely a voluntary storage mode.

The Ontario Student Record (OSR) is the ministry-authorized record maintained for each student in Ontario schools, from junior kindergarten to grade thirteen. The legislation defining these records creates a right of access to them for the pupil and for the parent or guardian if the pupil is a minor, and restricts third party access severely.²

2 Ibid., s. 231.

Prior to 1972, access to the record was at the option of the principal, who is and was responsible for the student record.³

Amendments to the legislation then governing school records⁴ created three categories of access rules. Teachers, principals and supervisory officers⁵ may see the records, which are defined as "privileged for the information and use"⁶ of these persons. The second category

3 An Act to Amend the Schools Administration Act, S.O. 1972, c. 77, s. 14.

4 Ibid.

5 The present Education Act, s. 1(1), paragraph 63, defines "supervisory officer" as:

a person who is qualified in accordance with the regulations governing supervisory officers and who is employed,

(i) by a board, or

(ii) in the Ministry and designated by the Minister

to perform such supervisory and administrative duties as are required of supervisory officers by this Act and the Regulations.

6 Section 231(2) of the Education Act, 1974 sets up a privileged status for pupil records thus:

(2) A record is privileged for the information and use of supervisory officers and the principal and teachers of the school for the improvement of instruction of the pupil, and such record,

(a) subject to subsections 3 and 5, is not available to any other person; and

(b) except for the purposes of subsection 5, is not admissible in evidence for any purpose in any trial, inquest, inquiry, examination, hearing or other proceeding, except to prove the establishment, maintenance, retention or transfer of the record,

(cont'd)

proscribes access to the record by all other persons, with two exceptions. A person designated by the Minister is allowed to conciliate disagreement between principal and pupil, parent or guardian about the record's content.⁷ The other exception provides the third access category whereby the pupil, and if the pupil is a minor, the parent or guardian, may access the record.⁸ Outside these three categories, no one may gain access to the pupil record without the written permission of the parent or guardian, or the pupil, if adult. The confidentiality of the record is further preserved by a requirement that "except as permitted under this section, every person shall preserve secrecy in respect of the content of a record"⁹

The practice concerning subject access appears not to have changed because of the legislation. We know of no case where a parent or pupil was refused access to his/her own record prior to the enactment; and no flood of requests to see the records has been perceived since the change. It is the practices in collection, maintenance and transfer of personal information which have been affected by the 1972

6 (cont'd)

without the written permission of the parent or guardian of the pupil or, where the pupil is an adult, the written permission of the pupil.

7 Education Act, 1974, S.O. 1974, c. 109, s. 231(5).

8 Ibid., s. 231(2).

9 Ibid., s. 231(10).

legislation. Its effects constitute the focus of our examination of student records.

1. What is the OSR?

The Pupil Record Regulation defines a pupil record to include:

- a) a record folder completed in accordance with this Regulation,
- b) achievement forms in respect of the pupil completed in accordance with this Regulation,
- c) documents, photographs, and information in writing inserted in the record folder with the approval of the principal,
- d) an index card ... and
- e) where the pupil is, on or after the 30th day of September, 1977, enrolled in a program of instruction in French as a second language, a record of French instruction completed in accordance with this Regulation.

10

The term "Ontario Student Record" (OSR) refers to all of these documents. With the exception of the Office Index Card, they may all be stored in the folder referred to in (a). The Office Index Card is, predictably, kept in the school office. The right of access applies to all of the documents. The form and content of each part of the OSR are prescribed by regulation.

The retention period varies for the different parts of the OSR. The achievement forms are kept for three years, and the documents, photographs and other insertions are kept only for one year. The rest of the record is to be retained by the school for 70 years after completion.

a) The Record Folder

The record folder is a file folder printed on all surfaces according to regulation. Part A contains identifying information about the student. It contains entries for the pupil's name, sex, birthdate, and a source of verification for this information -- a birth certificate, baptismal certificate, passport, or other such document. This part of the folder constitutes legal proof of age. We were informed that one of the main users of this proof of age form are persons reaching the age of 65 who need proof of age to qualify for pension benefits. Often this will be the only verification which they can produce.

There is a space for entry of the pupil's Social Insurance Number (SIN). The ministry manual on the use of the OSR states: "The Social Insurance Number may be added to the folder when it becomes known and available to the school." The ministry informs us, however, that any nine-digit number may be used. There is a preference for the SIN though, and while it is not mandatory, the ministry's memoranda expressing this preference have been worded in increasingly strong terms.

The use of the SIN for children who have not reached working age, who therefore are far from requiring it for its original statutory purpose, has elicited occasional but strenuous objection from parents.¹¹

Part B of the form records "schools" attended and "summary of progress." For years of schooling completed after 1974, an Achievement Form is placed in the file, and its number recorded in part B. Information concerning years completed prior to 1974 is also recorded in part B. This is the only portion of the old school record which is continued through the new form. Information categories in Part B consist of name of school, board and teacher contact as well as dates of entry and completion for each entry on the card.

Part C contains a more detailed summary of successful academic achievement, for secondary school purposes. It is divided into Communications, Social and Environment Studies, Pure and Applied

11 The case of Leise Shaver is perhaps the best documented example of such an objection. Her grade 12 teacher singled her out as the only one in the class who had not provided the number to the school. In fact, Ms. Shaver had never acquired a Social Insurance Number. Her father, enraged at the request that she obtain one for school record purposes, began his campaign of protest with the school principal and the local board of education. He continued through to the Ministry of Education, the provincial Ombudsman, the Premier, and his Members of provincial and federal Parliament. Ultimately he learned that any nine-digit number would satisfy the school computer's purposes. Leise Shaver was thus able to continue through school without a Social Insurance Number. Undoubtedly other students acquire the SIN for no other reason but the school record, even though they are not in fact required to do so.

Sciences, and Arts courses. With each entry under any of these categories goes the year the course was taken and date of completion, and the mark and credits achieved in the course. Only information pertaining to successfully completed courses is recorded here.

Part D records first names of parents, and their surnames if different from the pupil's name, or the guardian's name. The death of a parent or guardian is also recorded in this part.

Part E contains health information. Where the principal holds the opinion that a "special health problem" may interfere with a pupil's achievement, this information is recorded and updated annually, subject to mandatory consultation with parents or pupil. The parent or pupil's wishes in the matter need not be followed. The public health nurse in the school may or may not contribute to this information. Often, school personnel find that the information is not sufficiently detailed or current to be useful.

The date of the pupil's retirement "from school or from a private school to which his pupil record except the index card has been transferred" is the other mandatory information on the card. Parts F, G, H, I and K are for optional entry of the following information:

- . a photograph, with the date when it was taken;
- . extracurricular activity with dates;

- . "additional information" in the nature of referrals of the pupil to services or agencies, special talents or abilities, or anything else which may, "in the principal's opinion be beneficial to teachers in the instruction of the pupil";
- . outstanding achievements, awards or scholarships;
- . future employment or further education.

Part J indicates the date of "retirement" from the school system.

b) The Student Achievement Form

The second item enumerated as part of the OSR is the student achievement form (SAF). Form and content are prescribed by regulation.¹² The form sometimes requires a parental signature, to indicate that s/he has seen the form. This is not dictated by regulation, however. The SAF is sent home at least once a year, to keep parents apprised of the pupil's school progress. If a school is organized on a semester plan, the form is prepared at the end of each semester. Unlike other parts of the OSR which are retained by the school for 70 years, the Achievement Form is kept only for three years after the student retires from the school. This retention period is indicated on the form.

The purpose of the SAF is to report on the progress of the pupil. A school may design its own form containing statutorily prescribed elements and other information to suit the school's program. The form

¹² O/Reg. 38/75, s. 20.

will vary among schools, and at different grade levels. Little space is allowed for comment by the teacher. This contrasts with the pre-1973 forms, which could contain more commentary. A record of days absent and times late is usually shown on the form.

c) Miscellaneous Documents

The third category of item within the definition of the OSR is "documents, photographs and information in writing inserted in the record folder with the approval of the principal." Insertions in this category vary from school to school, and rarely do all folders in any one school contain all possible items. In some schools, psychologists' reports and standardized test results fall into this category; in others, notes of interviews with parents fit the description. As a matter of practice, teachers often purge the file of outdated material of this nature on an annual basis.

d) The Index Card

The index card comprises part of the OSR but is not kept in the folder. It bears "directory information" about the pupil including Social Insurance Number, information enabling contact with the parent or guardian, and previous schools attended by the pupil. Confidentiality concerns affect the policy of keeping this information separate from

the rest of the OSR, but teachers claiming a "need to know" the information sometimes find it inconvenient to call the office in order, for example, to contact a parent. They would prefer to keep this information in the classroom. The regulation was recently amended to allow the address to appear on the OSC.¹³

e) Record of French Instruction

The fifth form included in the definition of OSR is the student record of Accumulated Instruction in French as a Second Language. This form was added to the OSR in the school year 1977-78, by amendment to the regulation.¹⁴ It is found in the folders only of those students enrolled in a program with French as a second language, since September, 1977. The form covers courses from levels of junior kindergarten to grade thirteen.

2. Legislated Access to the Record

In addition to defining the details of the Ontario Student Record, legislation first passed in 1972 formalizes the record's purpose and

13 O/Reg. 911/78.

14 O/Reg. 610/78, s. 3.

the rights of access to it.¹⁵ Section 231 of The Education Act, 1974 now deals with access to records, defined broadly as those "maintained or retained by the principal of the school in accordance with the regulations," and is

privileged for the information and use of supervisory officers and the principal and teachers of the school for the improvement of instruction of the pupil.

The parent or pupil has a right to examine the record. It is not available to any other person without the consent of the parent or guardian, or pupil if adult. Further, the content of the record is not admissible in evidence in judicial or other proceedings without permission.¹⁶ However, it may be introduced in evidence to prove its "establishment, maintenance, retention or transfer" without such permission.¹⁷

In addition to establishing these strict limitations on access and transfer practices for pupil records, section 231 sets out a dispute resolution mechanism. An adult pupil or the pupil's parent or guardian may request in writing that the principal correct an "alleged inaccuracy" or remove "impugned information" on the grounds that the information is "not conducive to the improvement of instruction of the pupil." If the principal refuses to comply with such a request, the supervisory

15 Schools Administration Act, S.O. 1972, c. 77, s. 14.

16 Parr et al. v. Batkovich (1977) 20 O.R. (2d) 491.

17 Education Act, 1974, S.O. 1974, c. 109, s. 231(2) (b).

officer has some adjudicative powers either to compel compliance or refer the request to a hearing presided over by a nominee of the Minister of Education.¹⁸

Having given the record subject these procedures to assure protection of his/her interest, section 231 protects those who contribute information by stating that

no action shall be brought against any person in respect of the content of a record.

19

a) History of the Legislative Change

In 1972 the Schools Administration Act was amended by the access provision now contained in the Education Act, 1974. The 1978 revision of the "Manual for the Ontario Student Record System" describes the change in this way:

Because of the capacity of modern technology to provide instant communication of information, the permanent storage and the communication of data and records of acts or events threaten our privacy. The legislation concerning student records is the result of societal demands for a careful application of controls to guarantee a greater degree of privacy to students and their families than exists at present.

18 Supra, note 7.

19 Education Act, 1974, S.O. 1974, c. 109, s. 231(8).

The legislative change came about as a result of concern for the use made of pupil records both in the U.S. and Canada, reflected in civil suits brought against the school boards for record-keeping processes. According to one of the drafters of the Ontario section, the local case which spurred the change was one in which a secondary school student was criminally charged in a gun-shooting incident. The pupil's record was used by the prosecution to demonstrate to the court that the pupil had a bad record, including truancy and acts of delinquency at the school. The pupil never had the opportunity to know of the record's compilation. The stated legislative purpose for the record and the authority for collecting information in the first place was limited to the "improvement of instruction of the pupil." Its use as evidence against the pupil in the judicial process had not been contemplated. Understandably, concern was generated over the use of detailed personal information in a context other than that for which it was collected.

Other instances in which the pupil record had been sought occurred in certain hiring processes (for example, in reviewing applications for police officers or members of the armed forces) and in custody disputes. Largely to protect the school boards and individual teachers and principals from civil suits stemming from this type of record use, the ministry saw fit to amend the Education Act.²⁰

20 Telephone interview with Mr. L. Showler, Ministry of Education, Legal Branch, February, 1979.

In fact, although the ministry found that a steady flow of inquiries from parents worried about adverse pupil records was a factor in the passage of section 231, there have been remarkably few requests for access or change to the record since the amendment. Complaints about records have decreased in general. Section 231 appears to have achieved a greater trust in the record-keeping practices of schools.

From the teacher's point of view, there is some discontent with the legislated access rules. One Board of Education reports that some of its teachers have wanted to use pupil records as indications of the teacher's competence. Without pupil or parent permission, this is forbidden. However, the law does not contemplate release of pupil records which have been stripped of personal identifiers -- a solution to the problem which would apparently maintain the spirit of the law and provide the teacher with evidence of his/her working history.

A more common complaint is that teachers may no longer be entirely candid in pupil records, since pupils may object to their comments. The immunity to legal action granted by statute does not appear to resolve the concern. The result, according to teachers, is that they lack vital historical information to assist them in the classroom.

b) Current Record-Keeping Practice
with the OSR

The changes effected by section 231 can be observed in the actual record keeping practices of the schools, and their practices in relation to third-party requests for access. While the trend initiated by the Hall Dennis Report in the mid-60's was towards less emphasis on standardized achievement and more on individual fulfillment, the new OSR reflects very little of the idiosyncratic accomplishment of the child; it gives minimal and standardized information. The form itself allows for comment by the teacher in Part H. One educator describes this opportunity, however, as underutilized. The teacher's attitude towards the OSR has perhaps more influence on the record content than the form itself.

The following is a typical dialogue with a teacher on the subject of this change of record content.

Q: How has the information on the OSR changed?

A: It is more factual, objective, brief and generally less informative.

Q: Why?

A: With parent/pupil access now, we might be held responsible for what's on the record.

Q: Were they previously so damaging?

A: Actually only a small percentage of records contained possibly libellous information.

Q: Doesn't the statute protect you from legal action concerning the content of the record?

A: Yes.

Q: So why have the contents of the record been whitewashed in this way?

A: Well, it's how the ministry wants us to use the record.

This dialogue indicates that while the purpose of the new record form is to eliminate unnecessarily biased remarks, the impetus behind the change is due less to the teachers' interpretation of what is now appropriate, than to the ministry's guidelines on the subject. The fear of retribution or legal repercussions arising from a parent viewing the record has not been realized. The consensus of educators interviewed indicates that a very small percentage of teachers recorded improper remarks. They agreed too, though, that there was no justification for these remarks.

This is not to say that all subjective information is out of place on the pupil record. Many teachers expressed the view that especially at primary level, the educational process works best where the teacher has a maximum of information about the pupil. The information referred to here includes family and personal information which would not be reflected on the current forms, but which, in the opinions of these educators, falls into the statutory definition of record -- "for the improvement of instruction." An example was given of a child raised by a female single parent; it would be useful for a teacher to know of a father's absence so that additional male affection might be provided in the school context.

Teachers stressed that personal, especially family-related information is often recorded at a parent's request, and that even before the legislated right of access, parents most frequently saw the record at the teacher's urging. How far the teacher's role extends into assuming traditional parental responsibilities is a matter of some debate, and is a key issue in answering the question of how much personal information is required for improved instruction.

The attitude of the ministry towards material included in the OSR folder is illustrated by this advice contained in the current OSR Manual concerning "other information":

Any insert that is deemed to be conducive to the improvement of instruction may be placed in the OSR folder When deemed desirable, principals should inform social agencies such as the Children's Aid Society that their contributions are given full protection In this way, frank and complete reports could continue to be expected. However, these reports are subject to possible scrutiny by students and parents. 21
(emphasis added)

Administrators and educators acknowledge the utility of so-called "soft" information -- non-academic, personal, opinionative information. The prospect of subject access to records containing such information appears to act as a disincentive to the keeping of these records. This is despite the acknowledged relevance and utility of such records, the failure of parents and students to exercise their right of access, and the statutory protection from liability for teachers whose records are,

21 Manual for the Ontario Student Record System (Ministry of Education, Revised, 1978) 9.

in the rare case, found actionable. At this time we know of no case where a teacher has had to claim this protection.

One way to compensate for what some perceive to be the new record's inadequacy is oral communication among teachers. Our interviewees reported that it has always been customary for teachers to convey information about their pupils to subsequent teachers by word-of-mouth. These conversations have taken on added importance, as their substance may likely be information now considered out of place on the OSR folder. Teachers also mentioned that some keep "desk-drawer" notes, which do not become part of the official record but are useful in allowing a teacher to keep track of a pupil's daily progress. The teachers explained that these notes have no place in the OSR as they are not of permanent value, but do assist in the daily task of teaching. Such notes are outside the category of records for which a teacher may be held responsible.

3. Guidance and Psychological Reports

The practice concerning guidance and psychological reports varies from school to school. The function of psychologists and guidance counsellors is such that they must gather sensitive personal information. While records of this information may be "conducive to the improvement of instruction," as all information on the record must be by statute,

teachers no longer enter this type of sensitive information on the OSR folder. The following section examines the practices of psychologists and guidance counsellors in keeping their records.

Guidance counsellors indicated to us that although they are part of the teaching staff of a school, their records are often kept separately from the OSR. They are considered as the counsellor's personal files, not subject to section 231 of the Education Act, and accordingly not part of the pupil's official school record. The practice seems to be that guidance counsellors do not in fact keep records about their interviews with pupils. Many guidance counsellors make short notes of important decisions made during an interview, and place them in the OSR. The subject matter of the interview may concern academic, personal or family problems. It is psychologists, however, who appear to deal with the more serious problems of students, which in previous years were aired in the guidance office.

Psychologists' reports raise different concerns with respect to the confidentiality issue. There is the question of whether psychologists may have access to the OSR and whether teachers may have access to psychologists' reports, without corresponding parental consents. There is some question as to whether psychologists belong to the category of persons named in section 231(1) and (2) as record-keepers for whose access the record is privileged. Psychologists in schools are qualified as teachers, regardless of title. A regulation now stipulates that in

schools, professional support staff (e.g., psychologists) perform their duties subject to the administrative authority of the principal.²²

Different boards of education interpret the legislation in diverse ways. In fact, current practice by psychologists eliminates at the outset any potential parental objection to records containing sensitive information. Before a psychological test is conducted or a report made, parental consent is obtained. Where the student is over age 16, the student's consent is obtained; no parental consent is required. This is considered ethical conduct by the professional association of psychologists (the Ontario Board of Examiners in Psychology). In addition, parental consent, if required, may be obtained to permit the psychologist access to the OSR. The parent (or student) is consulted throughout the process, to keep him/her informed of the purpose, nature and results of the test. Thus, the parent or pupil does retain some control over reports in which possibly objectionable material may be contained.

Many educators believe that because the parent is informed of the substance of psychological records as they are compiled, the prospect of parental access does not represent the same threat for psychologists as it appears to do for teachers in relation to other accessible records. In addition, the parents or pupil may give a consent allowing

22 O/Reg. 704/78, s. 23.

the psychologist access to other school records. Thus, the technical problem of a psychologist's access under the legislation becomes irrelevant.

In many schools these problems of statutory interpretation do not exist, in theory or practice. At some schools, a psychologist is designated as a "psychoeducational consultant," at others as a "teacher diagnostician," in an attempt to confer the statutory status necessary to access records. In many instances, the psychologist has teaching qualifications, and by law has the same access to the OSR as others named by statute. Some psychologists obtain permission directly from the pupil or parent, while others are permitted at the principal's discretion to see parts of the record.

The confidentiality problem with psychological reports involves teachers who have access to the OSR. Psychologists' reports contain candid views and highly personal information, the type which was considered inappropriate in the OSR when placed there by teachers. Two rationales emerge for the conclusion of impropriety in the latter case. One is the "self-fulfilling prophecy" effect of commentaries placed on student records, whereby regardless of timeliness or accuracy, it is possible for a teacher reading such information to behave toward the pupil in such a way as to encourage the comments to become true. The second rationale simply considers it outside a teacher's proper role to collect or act on this type of information.

Unlike the more theoretical problems of statutory interpretation which are handled in various ways, a very real problem of improper access to psychological records may arise if a psychologist also enjoys the status of a teacher. This could mean that psychologists reports would become part of the OSR, thus giving access to other teachers.

Subjective, sensitive information is typical of the content of psychologists reports, and is the type of information which gave rise to the changed form and rules of access when teachers reports contained it. Does the expertise of psychologists eliminate the concerns attached to sensitive records which used to be compiled by others on the teaching staff? To the extent to which this type of information is compiled within the expertise of a psychologist, and used by the psychologist, the concerns are inapplicable.

The remaining concern, however, relates to the use of this type of information by non-specialists. Thus, when these reports are accessible to other teachers as part of the OSR, the problem remains. Teachers are not trained to interpret and apply the clinical observations of a psychologist. A problem may remain that teachers could misinterpret and misapply the observations of psychologists.

Some boards of education have attempted to solve this problem by inserting in the OSR only a brief summary of the psychologist's report in lay terms. Some boards remove psychologists' reports from a student's file before transferring it to a school under the jurisdiction

of another Board of Education. This remedy assumes that as long as the psychologist who wrote the report is available to interpret it, there is no danger of improper use of information in it.²³

Even in schools where psychologists reports are considered part of the OSR and even where the report is considered suitable for lay eyes, the report is often kept separately from the rest of the OSR, so that it is not readily available to a teacher. From the psychologist's point of view, the problem most commonly encountered (notwithstanding all the procedures described here) is the attitude taken by the board of education whereby as the employer, it owns all information compiled by the psychologist. It may claim desk drawer notes and raw test results as its property in addition to the report submitted by the psychologist. The absence of clear standards of practice and ethical guidelines and

- 23 The question of whether psychologists records belong to the employer school board or to the employee psychologist came before the courts recently, but was not resolved. The Ontario Board of Examiners in Psychology stated its position thus in its Brief of May 1979 to the Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario:

Psychologists had always assumed that on leaving the employ of a school board, their files would stay behind in the possession and under the control of the psychologists who succeeded them.

When the Lakehead Board of Education in 1977 ceased to employ any psychologist, and the last departing psychologist entrusted his files to a local children's agency under the direction of a registered psychologist, the Board commenced legal action to regain possession and control of the files. Although the issue was never decided by the court, the Board succeeded in asserting its claim to the files without the supervision of an appropriate professional.

the absence of public or client pressure to recognize or uphold confidentiality in a psychologist-client relationship leaves these problems unresolved.

4. Medical Records

Similar considerations feed a problem in the matter of medical records in the schools. There are two types of medical records maintained in schools. One is on the OSR folder. The other is the record maintained by the school nurse. While the common assumption is that medical information collected within the school context is intended for use by the school, the nature of medical reports and the professional standards of doctors and nurses betray the assumption. Teachers, principals, supervisory officers and parents may not be allowed ready access to these records, according to the medical profession. Nonetheless, there is some medical information which is needed in order that schools acquit themselves properly of the task of caring for so many children.

Medical information on the OSR folder, part E, is to be entered after consultation with the parents. Their consent is not required. Often it is a condition such as epilepsy which a parent may not wish to see recorded. As with impressionistic or otherwise sensitive information, there is a fear that the recording of the information conditions the teacher's behaviour toward the child and makes the possible negative repercussions of the child's condition a self-fulfilling prophecy.

Where medical information is recorded here, it must be reviewed annually in order not to keep stale information in circulation. Most commonly it is information concerning a hearing or sight condition which affects classroom performance. Often a teacher discovers this type of information directly from a pupil, as some teachers do not use the OSR to inform themselves of such matters. The comment from teachers in this connection is that the OSR is not sufficiently detailed to merit perusal of a classroom's worth of folders.

The school nurse is in fact a public health nurse in the employ of the Ministry of Health. In most jurisdictions, the sharing of information in the nurse's records with teachers has been considered crucial to the maintenance of proper measures to ensure the health and safety of the school population. It is customary in many schools for a conference to be held between teachers and nurse, to inform teachers of medical conditions of new pupils which may affect school activities. Most important is information transmitted to physical education teachers. The general practice would be that no diagnostic information would be transmitted, but merely symptomatic material for practical application in classroom situations.

This climate of easy exchange of information has been altered dramatically in the City of Toronto by the actions of the City's Medical Officer of Health, to whom all public health nurses report. Pursuant to the opinion rendered upon his request by the College of

Physicians and Surgeons, all records kept by public health nurses are now seen to be doctors records, and so a doctor's duty of confidentiality, not a nurse's, applies to these records. While nurses have discretion to discuss information which they receive in the course of their professional duties, doctors are bound to obtain the patient's consent to release such information. School nurses records are deemed to be doctors' records in some cases because their contents may have been communicated to the nurse by the pupil's doctor, and in any case because the Medical Officer of Health is the official custodian of the records.²⁴ The argument that the school stands "in loco parentis" to the student in respect of authorizing release of medical information to itself was rejected by the city's Legal Department, which closed off another argument to allow free flow of medical information between nurse and teaching staff.²⁵

The result in the schools is that nurses are under orders not to share their information with teachers. Interviews conducted among schools in Toronto indicate that there is compliance on the part of nurses, but nurses and teachers alike fear for the safety of their charges. In some schools, the nurse may indicate to a physical education teacher

24 Correspondence between Dr. G.W.O. Moss, Medical Officer of Health, City of Toronto, and Dr. H.W. Henderson, Deputy Registrar, College of Physicians and Surgeons, dated June 20, 1978 and August 14, 1978.

25 Opinion of City of Toronto Legal Department for Local Board of Health, dated January 25, 1979.

that a pupil is "restricted" from certain activities. The medical condition underlying the restriction is not described. One school nurse stated that she conducts discreet conversations with teachers who should in her opinion be aware of a pupil's disability.

The city plans to have a release signed by parents at the beginning of each school year, to restore the flow of medical information to teachers. Educators fear that this will be difficult to achieve. Although the administrative task is comparable to the burden imposed on the schools in obtaining parental permission for other matters such as field trips, some teachers express the view that parents may be unwilling to "sign away" such a right. High school students, they say, may actively avoid obtaining such a release. Contents of high school students files may include highly sensitive information concerning sex and drugs. At present some of the most compelling stories making the case against teacher access to nurses files involve teachers misusing information about abortion, or reporting drug use to the police. The pupil's confiding of such information to medical personnel anticipates that such information is used only to provide proper medical care while the pupil is engaged in activities under the jurisdiction of the schools.

In most other boards of education, nurses continue to share information, as they deem necessary, with appropriate school staff. However, parental authorization is required for the release of the nurse's record per se.

5. Other Contributors or Users
of a Student's Record

Social workers and probation officers sometimes have occasion to exchange information with the schools. While some schools use the vice-principal to supervise attendance and truancy matters, others employ social workers. In the City of Toronto these people are designated "special services workers." One school indicated that as parents may be held legally liable for their children's absence from school when it reaches truant proportions, parental permission is not required in order that special service personnel may have access to attendance records. To require it might be self-defeating. Similarly, while parental consent is needed before a psychological report is undertaken, no consent is required for a social worker's report. However, special services personnel have no legal right of access to the pupil record. The practice of preparing reports without parental consent may not be universal. One school reported a particular incident in which a social worker, having counselled a 15-year-old on her right to leave home at age 16, was subsequently threatened by the parents. Since that time, the school has sought permission prior to consultation.

All schools surveyed indicated that special service reports are stored centrally, with the board of education. If a student transfers to another school, the report which was returned to the school is transferred with the rest of the record. As with psychological reports, if a student transfers to the jurisdiction of another board, the report

may also be transferred, but the preference is that a consultation or written explanatory note accompany it. If a teacher wishes to see a special services report, most schools require the author to interpret it for the teacher. Some boards are reluctant to transfer a special services record to a school under the jurisdiction of another board of education because, in the absence of communication between the report's author and the new teacher, the information may be misinterpreted.

Social workers from agencies such as Children's Aid often interact with schools in compiling their reports. While a CAS worker is outside the definition of those having access to school records, teachers or principals may discuss a pupil verbally with the worker. One educator said that the criterion for confidentiality or discussion in this informal context was the best interest of the child. Others doubt that this is a legally defensible position.

Similar to these requests for information about pupils are lawyers' inquiries in the context of marital and custody disputes. The rule seems strictly enforced in this context, and schools do not divulge this information. There seems to be a preference given to agency workers over legal representatives in the policy for release of privileged student information, although the issue is generally the same: are the parent(s) caring properly for the child?

There is a regular flow of students between public schools and correctional institutions -- "training schools," which are within the jurisdiction of the Ministry of Correctional Services. The liaison for purposes of proper information exchange is made by a school supervisory officer, who has access to the school records. Generally, material compiled at a training school is not included in the OSR upon the student's return to the school system. The prejudicial potential of the mere fact of such a sojourn is clear. Placement forms accompanying the student on his/her return contain very sensitive material which may allow a school to determine whether to accept a child with a juvenile criminal record. There is a general responsibility on schools to educate eligible pupils, but a school may refuse to enrol a pupil for reasons of safety. The form is clearly marked "NOT TO BE PLACED IN OSR." The school principal has discretion to remove material from the record which may be detrimental to the student, and discretion is frequently exercised in this respect. However, Part B of the OSR folder which summarizes the student's successful secondary school achievement, may indicate that a student has spent time in such an institution, either because the name of the school is mentioned, or because a gap appears for that period of time.

6. Third Party Inquiries

Apart from the social service, correctional and marital dispute type of inquiries addressed to schools about students, credit-granting agencies and prospective employers are the most common seekers of information from schools about pupils. No information whatsoever is released over the telephone. If a student wishes to give the information seeker access to school records, a form must be completed, either by the student or his/her parent if the student is a minor. Some boards of education have devised standard forms on which to transmit the requested information. The rate of inquiries of this nature is said to have dropped somewhat since the changes to the school record, because the recorded information which may be released is so limited that inquiring parties do not find it particularly useful. Knowing only the attendance record of someone in high school is unlikely to be a secure basis upon which to grant credit. On the other hand, the type of subjective evaluation which may have been released previously in response to such inquiries was, at best, no more reliable.

One final category of inquirers should be identified. These are older citizens who, upon reaching age 65, wish to receive pension benefits and must establish legal proof of age. Especially for those born outside of Canada, and for women who have never worked or otherwise been in contact with official bureaucracies, the school record is their only legal proof of age. A steady though not voluminous flow of

inquiries is received from this group, which indicates the importance of the 70-year retention period.

7. Student Identification Numbers

The OSR folder contains a space labelled "Social Insurance Number." Although these numbers are elicited, they are not in fact required on the record, and ministry and school officials regard the item as optional. The Manual for the Ontario Student Record System states:

The Social Insurance Number may be added to the folder when it becomes known and available to the school. 26

Board of Education officials in the City of Toronto indicate that a nine-digit number is assigned to pupils for internal purposes from their central facility. If and when a Social Insurance Number is obtained, it may replace the previous number on the folder. However, the grade 13 master file maintained by the ministry uses Social Insurance Numbers if at all possible, as this tape is used for college and university entrance purposes, a system which requires Social Insurance Numbers as identifiers. Again, however, it seems that any nine-digit number will suffice.

C. Teacher Records

1. Description

The official records for teachers practising within the Ontario school system are held by the ministry in its Information, Systems and Records Branch. The contents of these records have been summarized by the ministry together with the current access policy as follows:

The Ministry considers the teachers' files maintained in the Information Systems and Records Branch as the official teachers' records. All material pertaining to a Board of Reference or disciplinary action will be incorporated in the respective teacher's file. All material pertaining to a person's application for the Supervisory Officers' examination will be incorporated in the respective teacher's file. Any person who has applied for certification or who is a qualified teacher in Ontario will have controlled access to his or her own record. No information, other than confirmation of certification held, will be made available to a third party, unless the third party has a right in law, without the written authorization of the teacher concerned ... Extraneous information that is considered subjective in nature should not form a part of the teacher's record. 27

Essentially, ministry-held teachers files consist of proof of certification, since the ministry is the certifier and not the employer. Local school boards, as employers, hold conventional personnel-type records about teachers.

Unlike pupil records, teachers' employment records are not governed by a section in the Education Act permitting access to and correction of

material on file. When the access provision for pupil records was being drafted, there was an unsuccessful move on the part of teachers to achieve a similar right. Access continues to be governed by collective agreement, and accordingly the practice differs across the province since agreements are reached with individual boards as separate employers.

The official certification record held by the ministry for a teacher, consists of Social Insurance Number, sex, date of birth, credentials, and nature and status of teaching certificates held. A certificate may be active, interim, cancelled, or suspended. This file may be accessed by boards of education engaged in hiring teachers, and for that matter by the general public, in keeping with the ministry's position that the status of teachers is of public interest, as the public has a right to know that teachers are qualified.

Evaluation reports about the performance of individual teachers are kept by local boards in what are known as "correspondence files." Until 1968, the ministry was directly responsible for the inspectors who assessed teachers' performance on a regular basis. An assessment letter or appraisal was placed on file as a result of the inspection. Since 1969, the ministry has used inspectors only for boards in the north of the province, which leaves approximately 75% of school boards to employ their own "supervisory officers." This change reflects the ministry's belief that a person more closely involved with the community can better assess the qualifications of a teacher for a position.

As a result of allowing teachers greater access to their own files, and because of the decentralization of teacher supervisory reports, the ministry has pared down its holdings of subjective material about teachers. Although the 1972 amendment to the Education Act allowing pupils access to their records did not officially affect records kept about teachers, a new spirit regarding personal records emerged. Old records were purged of subjective, non-factual material; thus the amount of subjective material collected or held about teachers by boards or the ministry has been greatly reduced. There arose a consciousness that teachers had a right to know what material was being collected about them for future determinations concerning their careers. Collection of material which could have no bearing on a teacher's performance or future employment was discouraged, and the consensus indicates that such collection has in fact decreased.

An innovation in record-keeping implemented by many boards is the practice of having a teacher sign evaluation or appraisal reports prepared by supervisory officers, before they are placed on file. Principals are required to advise teachers in writing within three days of any adverse comment being made to the file. Apparently, the threat of a negative letter to file has become more important in recent times, as budgetary constraints upon schools may result in the firing of teachers. The significance of the correspondence file, which contains the record on which a teacher's performance is appraised, has therefore taken on new meaning.

A practice urged by teachers federations, but not recognized in legislation or collective agreements, is the written response by teachers to reports considered inaccurate. In this way, if informal means of changing the record are not successful, and in the absence of codified methods of ensuring accurate records, a teacher may at least have on the record his/her response to the behaviour or incident in question. Thus, the danger of an unfairly prejudiced decision being made on the basis of such information is diminished.

The latest development in legislation concerning teachers is the promulgation in July, 1978 of Regulation 191 to the Education Act.²⁸ It sets out the principal's duties in terminating a teacher's contract. A principal must now give a warning to the teacher before action is taken to fire him/her. Assistance must be offered, and a reasonable time allowed for improvement.

At present, the retention period for evaluative material concerning teachers is an area of teacher discontent. One teachers federation affiliate wants a limitation of three years placed on the retention of evaluations. Since there is no opportunity for the old records to be updated, negative comments which are not currently valid may remain on the record, where they may be unfairly prejudicial to the teacher. No collective agreement governs this aspect of compilation and retention of records.

28 O/Reg. 191/78.

The main purpose of the correspondence file is for disciplinary action, and for a Board of Reference -- a hearing which the Minister may grant if a teacher's contract is terminated "in a manner not agreeable" to one party. There is a statutory requirement²⁹ that the termination of a contract by either party must be by notice in writing in accordance with the contract. If a board of education terminates a contract, reasons must be given. If a Board of Reference is held, the Minister ultimately receives a report on whether the dismissal was procedurally correct. In most Boards of Reference, it is an aggrieved teacher who disputes the propriety of grounds for firing. The significance of accurate records is evident in this situation. In fact, very few dismissal disputes result in Boards of Reference. According to the ministry, only seven to ten hearings may be held during a year. Nonetheless, material in the correspondence file may also be used at less formal proceedings to determine a teacher's continued employment.

2. Access to Teachers' Files

The formal provisions governing teachers' access to their own records are found in collective agreements. As mentioned earlier, the legislative reforms of a few years ago changed access for pupils but did not affect teacher records. Some collective agreements make

29 Education Act, 1974, S.O. 1974, c. 109, s. 233(1).

varying provisions for access, but most do not include any allusion to access whatsoever.

The City of Toronto makes extensive provision for access. A teacher must make a written request for an appointment, upon which s/he may "inspect" all information in his/her personnel file. The teacher may make a copy of such information, and may be accompanied by another person, although a written request to have such person present must be made in advance. If the teacher disputes in writing the accuracy or completeness of information in the file, the board is obliged to respond "in writing," within 15 days where possible. If an amendment to the file results, the board attempts to notify all those who received reports containing the inaccurate information.

The agreement with Etobicoke states only that a teacher may arrange an appointment by written request to examine his/her "record file." A supervisory officer must be present.

The North York Board stipulates that a prior request be made to see the personal file, but it need not be in writing. A supervisory officer must be present. An additional source of information, the "personal in-school data file," is made available. A teacher has a right to copy, and may see and sign evaluative materials placed on file. If a teacher refuses to sign, that fact shall be "stated on the material and placed on file."

A comparison of the three collective agreements illustrates the range of details which may be considered necessary for full access, from the point of view of the data subject and the record-keeper. The material which may be seen seems to vary from board to board; whether this is a question of semantics or whether content varies too is unclear. Teachers have protested the requirement of an appointment to see their files, for they fear it allows a record to be changed; yet all three agreements require some type of notice. The Toronto Board specifies that another person of the teacher's choosing may view the file with the teacher; the other Boards require in effect their own representatives to be present and make no mention of another of the teacher's choosing. Permission for this would likely depend on the individual school.

Correction of material on file is alluded to only in the Toronto agreement, but the complete process for disputed material is not set out. However, the North York agreement recognizes the significance of accurate records at an earlier stage than Toronto. In North York, a teacher has an opportunity to view material comprising the most sensitive part of the file before it goes on file. Thus, no teacher can say that decisions were made about him/her on the basis of material of which s/he had no knowledge. Presently, this practice is prescribed by a Code of Ethics. Its inclusion in the North York collective agreement indicates that the practice needs such additional reinforcement.

3. Conclusions

The discrepancies among the contractual access sections and the fact that only a minority of boards have an access clause in their collective agreements indicate a need for some uniformity. A committee formed by the Ministry of Education reported in June, 1977 that "controlled access" to the record should be granted to qualified teachers and applicants for certification, and that uniformity in maintaining teachers' records would be desirable. Certainly, it would be preferable to the current situation, where in fact approximately the same conditions may prevail in most schools for the viewing and maintenance of records in that access is rarely requested and when it is, an arrangement is made. We did not hear of any case in which access to a teacher's file was requested and refused. However, tensions exist because of the uncertainty as to how records are treated, and as the number of teaching positions decreases, this tension increases. Further, the tendency to set out access rights is growing. In the absence of guidelines, as the three agreements examined above illustrate, inequities from board to board may become entrenched. It seems to us that it would be better to establish a good practice at the outset than to re-examine a hodge-podge of solutions to the same problem after the practices become set.

D. Universities, Colleges and
Trade Certification

1. Description

The Ministry of Colleges and Universities is responsible for administering capital and operating grants to universities and colleges in the province, financial assistance to students, and certain programs relating to trade certification and training. The majority of records kept by the ministry deals with financial and physical plant information. Most records relating to individuals in the post-secondary educational context are kept at the university or college where the student is enrolled. The major exceptions are student awards records and industrial training program records. Student award records are maintained at the institution from which the student applies and at the ministry, which is responsible for the decision to grant an award. Records are kept about industrial training course enrollees for two purposes. Because these courses lead to certification in trades, certain ministry-set requirements must be met. In addition, since tuition and living allowance is paid by Canada Manpower, there is a need for accountability.

2. Industrial Training and Trade Certification Records

The Industrial Training Program was at one time under the jurisdiction of the Ministry of Labour. Now it is included as a program of the Ministry of Colleges and Universities. The two ministries reflect the two main aspects of the program's purpose: the certification and training of tradesmen. The training programs for certified trades are chiefly carried out at community colleges, and most are connected with federally-sponsored programs under Canada manpower. Living allowances are provided for trainees who qualify under the joint federal-provincial plan.

Students in industrial training courses must be at least one year over school-leaving age (17 in Ontario) and not have been in attendance for at least 12 months since leaving school. They must be referred to a program by Canada Manpower. A 1974 survey indicated that 66.4% of these students in Ontario were unemployed prior to entering the program, and only 24% had achieved high school graduation or a higher level of education.³⁰

The provincial legislation regulating certified trades is the Apprenticeship and Tradesmen's Qualification Act.³¹ Its regulations

30 Ontario Federation of Students, "The Training Game: Canada Manpower Training Program in Ontario" (Monograph, September 15, 1977) 2.

31 R.S.O. 1970, c. 24 as amended.

govern 35 trades in which every worker except an apprentice must hold "a subsisting certificate of qualification in the certified trade."³² An apprentice is defined as "a person who is at least 16 years of age and who has entered into a contract under which he is to receive, from or through his employer, training and instruction in a trade."³³ The regulation governing each trade sets out the course of classroom and practical training and the scale of wages to be paid during each period of training and instruction. The general regulation³⁴ under the Act prescribes that an applicant for apprenticeship may be required to produce a birth certificate or other proof of birth, as set out by regulation. The Director of Apprenticeship is empowered to prescribe examinations, issue certificates of apprenticeship³⁵ and similarly prescribe examinations and issue certificates of qualification. The Director may issue certificates of qualification without examination or apprenticeship under certain conditions and has the power to suspend or cancel certificates upon a hearing according to the rules of natural justice set out by section 24 of the regulation.

The Industrial Training Branch has its administrative function performed at the Queen's Park offices. Dealings with industrial

32 Ibid., s. 10(2).

33 Ibid., s. 1(a).

34 R.R.O. 1970, Reg. 33.

35 Ibid., s. 14.

training applicants and students are conducted through nine district offices each with a resident district supervisor, and thirteen local offices, which are run by clerical staff and apprenticeship counsellors. These field offices receive applications, administer examinations, and determine the eligibility of candidates for programs and for certification. Generally, they administer client services.

In the course of training, apprenticeship, examination, qualification and the continuing regulation of trades, a great deal of information is collected in relation both to the training program and to the individual. Some of it is specifically for the federal government -- a schedule of training days per course must be compiled in order to receive federal funding. There may be audit checks run from time to time to account for how many students are at which colleges, in which courses, during what time periods. None of this information includes personally identifiable material; however, there may also be inter-provincial transfers of information concerning individuals granted upon an individual's written consent or request, often in the context of a tradesman changing residence. A status report about an individual's completed training is requested in order to certify that individual in the trade in another province.

There is regular exchange of information with the industry for which the college trains individuals. The presence of an industry in an area often causes a training program to be established. Currently, there

are 314 non-regulated trades and 35 regulated trades in the province for which training schedules have been approved. In both cases, the impetus for setting standards often emanates from the private sector.

In the non-regulated trades, the industry concerned submits a schedule of training requirements for the ministry's approval, and an in-plant or college training schedule may then be set up. Training requirements for regulated trades may or may not be mandatory for employment in the field, but the training course is set by the Provincial Advisory Committee, which is composed of "equal numbers of representatives of employers and of employees and the Director"³⁶ of Industrial Training, or his/her appointee. In both regulated and non-regulated trades, examinations are set and hours of on-job and classroom training must be completed for certificates of apprenticeship. In regulated trades only wages are set by regulation during the apprenticeship period. The course of training and apprenticeship for regulated trades culminates in a certificate of qualification; again, this is not the case for non-regulated trades. In both instances though, employers seek employees through the courses. As the participation of Canada Manpower suggests, a goal of the Industrial Training Branch is not only the training but also the placement of tradesmen.

36 Ibid., s. 3(1), (2).

Private industry is in regular communication with the branch to establish and conduct appropriate training courses, to oversee the completion of prescribed training hours, and to assist those having completed their training in finding appropriate jobs. We were informed that in some communities the colleges are very open with prospective employers about information collected on trainees. The college staff consider themselves to be assisting the trainees in this way; they see it as part of their job. This is particularly true in communities dominated by one industry, where training programs are designed in conjunction with the industry. The records collected through training include information about previous education, and detailed performance and attendance reports from the course. Clearly, this information may assist the employer in choosing new employees. This employer use of the information collected is nowhere disclosed to students.

The records not only determine whether a student succeeds or fails in the particular course, but also affect:

- 1) his/her training allowance from Canada Manpower,
- 2) the rate of apprentice wage set by period in the regulated trades, and ultimately,
- 3) the rate of pay which may be commanded by a qualified tradesman.

The Ontario Federation of Students made the following comments about present living allowances and training courses:

Unlike post-secondary students and unionized workers, who cannot be expelled or fired without some form of appeal process, manpower students can be "terminated" for a whole range of

matters and the decision is not subject to appeal. Their living allowance is immediately cut off upon termination. 37

Reasons for termination range from absenteeism to an instructor's assessment of the student's attitude. This and other data is recorded by the counsellor, whose comments appear on the apprentice training evaluation form. Attendance seems to be a factor most consistently noted. This may be explained by the program's funding, which is based on the number of training days provided to a trainee. Consequently, the importance attached to attendance records may have considerable impact on the student.

Many of the records in the Industrial Training Branch are automated. The computerized files are indexed by name, trade, and Social Insurance Number. Their contents include details of past education and courses taken in the present program. These records have been automated for about 10 years, and key-punching is still done at the Ministry of Labour.

Records containing information about fees paid and examination results are kept manually. The Branch has been rearranging file storage to improve physical security by establishing a closed file room with a retrieval system which utilizes file request slips. Through this system the whereabouts of a file will be known at all times. Also, the

approximately 29,000 alphabetically-indexed files on apprentices will be converted to indexing by SIN. A total of approximately 200,000 certified tradesmen are already on these records. A certified apprenticeship is recorded on microfilm, one month after it is achieved, and the corresponding hard copy is sent to the Cooksville Record Centre. All records on tape dating back to the program's inception in 1928 are stored at the Branch.

Applications to the program are currently stored automatically on a modular program which facilitates retrieval. Plans exist to install on-line access terminals at the 28 local branch offices across the province.

3. Subject Access

We were told that a dispute about any matter on file would be recorded. Since students in training programs and trade certification have no access whatsoever to ministry-held files, it is difficult to understand how they would become aware of a matter for dispute.

In light of the relatively high rate of information exchange with others than the data subject, and in view of the uses made of these records, it might be expected that individuals would be permitted access to their own records on request, to assure their accuracy and be aware of their contents. This is not the case,

however, and the opinion of ministry staff with whom we spoke in trade certification administration and training programs was that access should not be permitted. Perhaps this attitude stems from the fact that no access requests have been received; however it was also implied that record ownership rested with the branch, not the individual, and that permitting access by individual record subjects would simply raise problems. Presently, there is no written policy governing student access. Given the nature of the information contained in the records, and its use by persons outside the training program, and given the fact that such information could have a direct bearing on employment prospects and pay, we believe that the justification for permitting access is irrefutable.

4. Student Awards

The Student Awards Program is administered by the Ministry of Colleges and Universities for the purpose of distributing funds, on a grant or loan basis, to post-secondary students at Ontario universities and community colleges. The program currently consists of several plans -- Ontario Study Grant Plan, Canada Student Loans Plan, Ontario Student Loans Plan, and Ontario Special Bursary Plan at the undergraduate level, and Ontario Graduate Scholarships, Bursaries for Second Language Teachers and Fellowships for Second Language Study. As the names indicate, most of the plans administered through the ministry are provincially-funded. The Canada Student Loans Plan is federally-funded.

Application forms are completed by students requesting financial assistance, giving various data to determine eligibility. Criteria include work and study history, marital status, residency and citizenship, the duration and nature of the education program and the income available to the student. Since 1978, in addition to the basic application form, an "Approval for Release of Tax Information" and a "Statement of Assets" must be completed.

Student awards applications for all plans are received through the university or college Student Awards offices. The Ministry determines eligibility, but the university acts as liaison with the student. If an appeal is taken against the amount of an award, or against the refusal of an award, it is also done through university personnel. The file at the university contains much of the same information as the one compiled at the ministry. Data verification, however, is only carried out by the ministry, so that that material does not appear in the university files.

Student awards files are considered to be the property of the university; therefore access policy cannot be dictated by the ministry. Accordingly, it may vary from one institution to another. At the one major institution we surveyed, the attitude was that the university is the advocate of the student, thus the file is open to the student upon presentation of proper identification such as student card or Social Insurance Number. Access is rarely requested; however

if a student did ask to see a file, an officer of the institution's Awards Branch would be present to ensure the file's security and to answer any questions from the student. Most inquiries are for specific details and readily answered by the awards officer. Thus, the question of access to the entire file arises infrequently. It most often surfaces in the context of appeals, where again the practice permits access to the student in the presence of an awards officer.

Access to files is also rarely requested at the ministry, since most students deal with awards through the university or college awards officers. If a student cannot satisfy an access demand at the college or university level, it is likely to be a senior ministry representative who takes up the matter of a file with the unsatisfied applicant. The only information which may not be open to an applicant is a reference letter, which is filed in connection with graduate student awards. This exception is to protect third parties who provide references on assurance of confidentiality.

Information may be requested from the ministry by people other than those involved in the administration of student awards. Access is only granted upon the student's approval in writing. Usually this occurs within the context of litigation, marital disputes, or credit checks.

At the university level also, requests for information may come from third parties, and again the written authorization of the student is

required before any information is released. A special case involves university administrative personnel seeking tuition or residence payment. They only receive confirmation of a student's application for assistance, and are not provided with specific financial information.

If a student defaults on payments towards the student loan, information about this may be provided to banks or collection agencies acting on behalf of government, or to federal government representatives. Address, employment, or family information may be released in this way. Ministry officials interviewed felt that the warning on the application form that "It is an offence under The Canada Student Loans Act to give false information" indicated such potential release. We do not agree.

Once an application reaches the ministry, it is first sorted in an open area according to plan of award. Income information on the applications is relayed to computer tapes for storage. The hard copy is stored at the branch. Some additional information is collected by the ministry in the course of processing applications. Reference letters are solicited in connection with graduate scholarships and teaching certificates for Teachers Second Language Bursaries. Some credentials about previous second language training may be required in connection with second language bursaries for students.

This additional information is maintained as hard copy. Some security problems have been experienced in connection with processed applications

where unauthorized personnel have had access to documents. Regardless of whether or not harm resulted, such access was a breach of confidence in respect of the personal information maintained in these files. As a result, the Awards Branch recently relocated its office on a floor of the ministry where additional security measures could be implemented. This security measure has increased physical control over the files. The classification of files is now by Social Insurance Number, and not alphabetically by name. Only file-room personnel may enter and leave the area freely; they number sufficiently few that identification on sight is satisfactory. Anyone wishing to retrieve a file must produce some identification or be known to the file-room personnel. A "file request" form is filled out in triplicate by the file borrower; two copies remain with the file registry, and one is left in the file to be returned to the file registry if the file is transferred. In this way the location of a file is known at all times.

Unfortunately, the security measures surrounding unprocessed student award applications and other awards contrast sharply with those described for processed files. The applications sit in piles on tables in an open area of the offices. Although they are not sorted, and often lack some items of information, the opportunity for information pilferage is clearly present. Similarly, Graduate Student Awards applications, both processed and unprocessed, are stored in a filing cabinet outside the Registry, without the security of the system described above.

The storage of applications is of relatively little public concern, but the branch has become increasingly mindful of its security needs, if not on a consistent basis. What has raised considerable comment recently is the additional information elicited by the tax return waiver and declaration of assets.

The tax return waiver states that "all information obtained from tax returns and Revenue Canada will be treated in strictest confidence." The operative paragraph of the form, drafted by Revenue Canada to assure the confidential status of tax returns, enables the provincial ministry to receive "a copy of any portion of my (1977 and 1978) Income Tax Returns or data derived therefrom that specifically pertains to information given by me on this application for Ontario Student Assistance." This is followed by a statement of purpose (verification) and a statement prohibiting further disclosure "except where further investigation is required or except where legal action is required."

Information submitted to the federal government on the income tax return is considered highly confidential, and its official use has been perceived by the public as restricted. Prior to the institution of the tax return waiver, the Ministry of Colleges and Universities had used tax returns as a method of verifying income information on student awards applications on a basis of random selection. Since the awards are made on a "needs" basis, the accuracy of income data on the application is paramount in determining awards. However, in the past,

only self-employed persons routinely gave a release for income tax returns. If indications of abuse of the awards system were obtained, by a process of random checks or complaints of cheating, subjects of verification were asked to submit their tax returns. In this way, an error margin of 5-7% was perceived, and ostensibly corrected. Thus, the old verification system resulted in 5-7% of applications being refused awards, whereas these might have been granted on the basis of the application alone.

Now, a release for income tax records (tax return waiver) must be completed at the time an application is made. Efficiency is the stated purpose for this new system. One also suspects that budgetary restraint is behind the ministry's desire to pare down awards as much as possible, despite the surplus in the student awards budget over the past few years. As a result of the tax return waiver, income stated on the award application is recorded on computer tape, and the tape is then compared with a tape containing income information obtained from the tax return. A reconciliation tape results, and if a discrepancy is revealed, additional information from the tax return may be taken. However, the applicant is notified of the discrepancy first, and is asked to account for it.

It appears that due attention is in fact paid to the confidentiality of tax documents required for verification of student award applications. The main objection levied is that mandatory release of confidential

information is an unwarranted invasion of privacy. The honesty of applicants is automatically put into question. Opponents of the release form maintain that the "error margin" revealed by random checks in the past did not warrant this additional privacy-invasive technique. However, the result has been a drop in applications of 38% to 55% at midsummer of the first year of the waiver's use. Some would conclude that many applicants represented in this drop would have been fraudulent and thus the use of the waiver effectively reduces improper awards. In fairness to the general student population, the drop in applications represents many factors; for instance, the drop in university applicants, and changed criteria and amounts for student awards. However, as well as fraudulent applicants, the drop may reveal a percentage who feel that the intrusiveness of the application outweighs its favourable terms as a source of education financing.

The Statement of Assets has received similar criticism. It elicits personal information normally not on any other record, and no indication is given as to how the information is used, or by whom. No statement about the confidentiality to be maintained by the recipient of the information is made. Yet details about the student's (and/or parent's or spouse's) real estate investments, personal property and business holdings must be submitted.

Statistical data for planning, policy and budget projection purposes are compiled on the basis of applications and other information collected

through the awards data. Some information is shared with the federal government, as both the Secretary of State and Revenue Canada are involved in some of the plans. However, we were informed that personal identifiers are removed from all statistical data.

The retention period for computer tapes at the ministry is one year. The back-up hard copy is maintained for the duration of the student's stay at the institution, plus one year. Thereafter, it is sent to the Cooksville Record Centre. If a student re-enters the education system and applies for assistance, the old record may be retrieved, but in most cases it remains at Cooksville.

E. Conclusions

1) The experience with a statutory access scheme for pupil records in Ontario schools indicates that while the provision has not been widely utilized, there is some indication that it has responded to a publicly perceived need. The availability of files seems to have reassured the public of the propriety of record-keeping. On the other hand, teachers are less satisfied. They appear to resent the curtailment of some types of record-keeping; namely, impressionistic observations. Although ministry and supervisory officials state that room is provided for recording necessary sensitive information, and even though statutory immunity from civil actions protects teachers from recourse with respect

to the record, teachers nevertheless exhibit a desire to make their reports briefer and more objective. They find each other's reports less useful this way, but interpret the statute and directives as requiring the omission of such material.

2) Medical and psychological records kept in the schools raise difficult questions about the propriety, necessity and confidentiality of certain sensitive data in the schooling process. There is a clear need for teachers and supervisory staff to be aware of conditions affecting the student's well-being in class. In the absence of this information, the student's well-being may be at risk, and the teacher may be seen as responsible for mishaps without having been able to guard against them. On the other hand, unlimited access to medical information may overstep the bounds of the teacher-pupil relationship. The unclear status of the psychologist and the school nurse only add to the confusion. Some attention should be devoted to defining their proper roles at least insofar as this would lead to a clearer definition of status and hence access rights and prohibitions under the legislation.

3) No uniform policy exists for teachers in relation to their employment records. Although collective bargaining agreements include such a clause, it would be preferable that all teachers be given uniform rights of access to the documentation governing their working conditions.

4) In the matter of student awards, it would appear that access to files is primarily requested at the university or college level, i.e. outside the ministry's jurisdiction. However, this may give rise to an uneven access policy across the province to the same files, which may have a material effect on grants, appeals and subsequent applications. It would be desirable to institute a uniform access policy to be practiced by all institutions where students receive awards.

5) Tax returns have always been used by student awards officers to verify income information. Now, the practice is to release only the income amount and only on the computer tape which is run against the income amounts indicated on the student award application. Previously the entire tax return was required by the student awards branch if information required verification. However, despite the knowledge of the applicant of the fact of verification, and despite the attention given to the confidentiality of the information, the release of the tax return is mandatory for a student awards applicant. Whether it is truly necessary to access tax records at all is a question which we are not qualified to answer. However, assuming that the rate of improperly obtained awards in the past does merit this abrogation of privacy, the form of the tax return waiver should explicitly state the limits of the use and the extent of access to the tax return. Similarly, the Statement of Assets should state to the applicant the purpose of the information submitted, and indicate the extent to which that information may be used or accessed by persons outside the student awards administration.

6) Industrial Training records should be subject to access and correction by the trainee, and later, upon certification, by the tradesman. The extent of benefits depending upon record accuracy makes any other situation untenable. The lengthy retention period for many of these records is questionable. How long can a record of classroom or training performance be useful after a person has achieved certification in a trade? In our opinion, after a certain period there ceases to be a reason for retention.

7) The somewhat casual exchange of information in smaller centres between college and industry raises a concern for due attention to the expectations of privacy of the trainee. Although it may be in the best interest of the trainee that a potential employer be apprised of a potential employee, the information was not collected for that purpose. The data subject should be made aware of all possible uses of the records, and given an opportunity to verify them.

CHAPTER X

GOVERNMENT PERSONNEL RECORDS

A. Introduction

In its role as an employer, the province of Ontario needs to keep records on thousands of people who administer and operate government programs. In many respects, these records reflect the practices and problems of personnel management experienced by any major employer. A report published by the United States government suggests that the personal records about government employees are kept in the context of a relationship more intense than the usual relationship of a government to its citizens:

In employer-employee matters, government's involvement with the individual goes beyond the relationship of the constituted governing authority to the citizen. ¹

The government employs office clerks, highway engineers, chemists, police officers, computer experts, economists, drivers, doctors, teachers, and other categories of professional, skilled and unskilled workers.

This chapter will examine the personal information practices of the

1 Privacy: A Public Concern: A Resource Document, based on the proceedings of a Seminar on Privacy sponsored by the Domestic Council, Committee on the Right of Privacy and the Council of State Governments (K.S. Larsen, ed., Washington, D.C.: USGPO, 1975) 28.

government in its role as employer. It will focus on the types, collection, storage, maintenance, and transfer of information collected in this context. Questions of subject access and correction or dispute of the record will also be examined.

Our analysis is based on interviews with staff of the Civil Service Commission (CSC), the Employee Data Services Branch of the Ministry of Government Services which operates a government-wide computerized employee information system, the Employee Health Services Branch, and personnel directors and staff in selected ministries. In addition, we conducted a survey of personnel files held by all ministries in the Ontario government, by means of a questionnaire. To gain an outside perspective on personnel record-keeping by the government, we spoke with representatives of the Ontario Public Service Employees Union and the Canadian Union of Public Employees (Local 1750).

B. Organization of Employees

The Civil Service Commission is the body within the Ontario government which is responsible for administering The Public Service Act² and its regulations, which govern the employment of public servants in Ontario. The chairman of the Commission has the rank of a deputy minister ex

2 The Public Service Act, R.S.O. 1970, c. 386 as amended.

officio.³ In addition to the chairman, the Commission has six other members. It is supported by a staff of personnel administration specialists. Much of the day-to-day personnel administration is authorized by individual ministries, who deal directly with their employees, according to rules established by the CSC. Each ministry has a central personnel branch, and there may be some offices where ministry operations are geographically dispersed. There are two broad categories of employees within the Ontario Public Service: classified and unclassified.⁴ In practice, these terms relate mainly to the permanence of employment. Classified employees, of whom there were 68,481 on March 31, 1977,⁵ are appointed by the Civil Service Commission to their positions first as probationary staff for up to one year. Regular staff are appointed by the Lieutenant Governor in Council, upon certification by the Civil Service Commission.⁶

The unclassified civil service varies in size at different times of the year. It is appointed by the relevant minister, or someone delegated by him; not by the CSC.⁷ Appointments are generally for one year or less at a time, and usually for a total of no more than three years. There

3 Ibid., s. 4.

4 Ibid., s. 1(b), (i).

5 Interview with research staff, Ontario Public Service Employees Union, April 4, 1979.

6 The Public Service Act, R.S.O. 1970, c. 386 as amended, s. 7.

7 Ibid., s. 8.

are two groups of unclassified employees. Group 1 is typified by students on individual contracts, the temporary secretarial pool ("GO Temps"), staff working under 24 hours weekly, special or professional appointments, and staff for projects of a non-recurring kind. Group 2 employees are hired to fill seasonal positions, for instance, provincial park employees.⁸

There is another group of Crown employees; those who work for Crown agencies such as the Niagara Parks Commission, or the Workmen's Compensation Board. They are appointed under the legislation creating the agency and not by a ministry at large.⁹ Most of the provisions of The Public Service Act do not apply to these employees,¹⁰ thus while they are Crown employees, they are not included in the definition of civil servant.¹¹

8 O/Reg. 749, s. 5.

9 The Public Service Act, R.S.O. 1970, c. 386 as amended, s. 1(e). For example, The Arts Council Act provides for the appointment of its members directly by the Lieutenant Governor in Council; The Alcoholism and Drug Addiction Foundation Act authorizes the expenditure of funds for, inter alia, living staff.

10 While the more inclusive term "public servant" is utilized through some of the relevant legislation, where it or the term "civil servant" is used, some Crown employees are excluded. The Public Service Act, ss. 11, 12 and 15 dictates the political activities of Crown employees, and other working conditions are governed by The Crown Employees Collective Bargaining Act, S.O. 1972, c. 67 as amended.

11 The Public Service Act, R.S.O. 1970, c. 386 as amended, s. 1(a).

These groupings are significant for at least three reasons. First, they determine the application of policy. If an employee is appointed under an act, s/he is subject to very little of The Public Service Act. Second, the union to which an employee may belong is determined by the category. Third, some decisions as to the type of personnel records to be kept are determined by the category.

The regulations under The Crown Employees Collective Bargaining Act¹² establish the bargaining units. Most employees are included in the Ontario Public Service Employees Union; 50,000 of the total 67,000 civil servants.¹³ OPSEU includes all classified and unclassified employees, with the customary exceptions of management, student and special professional employees. Another major employee organization is the Canadian Union of Public Employees (CUPE), which represents approximately 1,800 employees in two locals.¹⁴ The 800 employees of the Addiction Research Foundation are presently organizing a bargaining unit in OPSEU.¹⁵ Over 10,000 community college teachers and support staff are included in OPSEU bargaining units, through The Colleges Collective Bargaining Act.¹⁶

12 The Crown Employees Collective Bargaining Act, S.O. 1972, c. 67.

13 Interview with research staff, Ontario Public Service Employees Union, April 4, 1979.

14 Ibid.

15 Ibid.

16 The Colleges Collective Bargaining Act, 1975, S.O. 1975, c. 74.

The designation of the employee is also significant in terms of involvement in the centralized personnel record data base, operated by the Ministry of Government Services on behalf of the Civil Service Commission and the ministries. This data base, which will be described in detail later in the chapter, is known as the Integrated Pay, Personnel and Employee Benefits System (IPPEBS). It brings together relevant employee data for all aspects of routine personnel administration. Ministries are obliged to participate in that system as far as their classified employees are concerned. Participation is optional for information concerning unclassified employees, who do not generally have an ongoing employment relationship with the government and do not have as many benefit entitlements.

Against the background of this brief sketch of the organization of personnel administrators within the Ontario government, we turn to an examination of personal information practices.

C. The Hiring Process

The initial stage of information collection takes place during the hiring process. A standard "application for employment" is used by the public service as a general recruitment tool. Other information for specific positions may be sought by the employer.

The general application was revised in June 1978. The major change is the bilingual presentation of the form. Other changes affect the presentation of questions more than their substance, but many may reflect a growing concern with so-called privacy interests. No longer are applicants asked for weight and height. A request to know "maiden/family name known to references" has been eliminated. Applicants are no longer asked whether they have use of a car. Now, the only health-related information on the form is requested in a manner which indicates the optional nature of the request.

In general, the purpose of the information elicited on the form is indicated, whereas on the previous form, the purpose of information once collected was not clear. Thus the new form states "to be eligible for employment, you must be a Canadian citizen or permanent resident," then asks the applicant's status. The wording on the old form was "entitled to work in Canada by reason of: Canadian citizen, landed immigrant status, work permit." The changes made to the application form reflect principles of privacy protection. The purpose of the information is indicated. Less personal information is required. In the case of "use of car," the question's elimination may reflect the limited usefulness of the information.

Similar motives may be ascribed to the disappearance of the weight and height inquiries. Their elimination is also in accordance with the privacy protection principle which avoids overly intrusive queries, separates medical from general information, and accords it special security if it is recorded.

Some changes on the new form are related to verification practices. The old form indicated that proof of education qualifications may be required. Our surveys of personnel officers indicated that in fact, the vast majority of ministries do not verify qualifications as a matter of course. The new form no longer alludes to verification. The section of the old form pertaining to employment history asked whether each previous employer could be approached for a reference. Now the form simply states that employers "may be approached for reference after interviews."

For some employment positions, subjective information gathered in the course of interviews is recorded. For example, in the case of applicants for positions with the Ontario Government Protective Service, the subjective assessment made during the course of an interview is recorded on a standard form, which requires the interviewer to rate the dress, neatness, facial features and complexion, voice, manner, enthusiasm and alertness of the applicant. Under dress, descriptive adjectives such as "conservative, ordinary, flashy, rural, smart or casual" are suggested. The hiring criterion of facial features depends on such factors as "skin: healthy, coarse, sallow, etc." While detailed recording of these assessments provides a documented rationale for the interviewer's recommendation as to suitability for employment in a position with a high public profile, the very recording of such information may cause concern. We were assured that the information is kept as highly confidential material, is not used in the consideration of applicants for other positions and is destroyed after one year. The use of such forms can

undoubtedly assist the interviewer in verbalizing general impressions about a candidate, which are invariably made in an interview setting. It enables the objective assessment of competing candidates. As the basis for subjective assessments of such attributes as neatness, confidence, attitude, etc., can change markedly within a short period, one-time assessments should not be used for future judgment about an individual. The return of such material to the applicant or its destruction as soon as it is no longer useful would prevent an abuse of personal information, which is at risk when one person's impressions are applied in another situation by another person.

1. Security Clearances

For some categories of jobs, more extensive information about the individual is gathered. Our survey revealed that security clearances are undertaken by the Security Branch of the Ontario Provincial Police (OPP) on applicants for positions in the Lieutenant Governor's Office, the Premier's Office, and various branches of the Ministry of the Solicitor General. Most security clearances performed by the Security Branch are in relation to applicants for civilian and uniformed positions within the OPP. Apart from security clearances, simple criminal record checks are undertaken on applicants for a variety of sensitive positions within other ministries. Requests for criminal record information are referred directly to the Central Records Branch of the OPP. This Branch stopped doing such checks itself recently, as

it could not guarantee the completeness and accuracy of its records. All criminal records are now ascertained by means of fingerprints sent to the Royal Canadian Mounted Police (RCMP). Ministries inquiring after criminal records include Housing, Natural Resources (conservation officers), Consumer and Commercial Relations (Ontario Securities Commission staff), Attorney General, Health (ambulance attendants), Community and Social Services (employees required to be bonded), and Corrections (which obtains criminal records directly from the RCMP).

There are two levels of security clearance which are carried out by the Security Branch. The first is the "high security clearance," which is performed on applicants for specified categories of jobs where the need for security is paramount. The person concerned is asked to sign a form giving consent to the security check. S/he is then asked to complete a personal history sheet which requires details as to nationality, marital status, relatives over the age of 16 (including brothers- and sisters-in-law and their wives or husbands), previous employers and occupations. Information is requested about criminal convictions (excluding minor traffic offences), and a set of fingerprints is taken. An investigation is then carried out by a member of the Branch. This starts with an interview of the subject to obtain background information on his/her hobbies, church attendance, club memberships and education. Questions are asked about the use of alcohol or drugs and about travel, particularly to communist countries. The investigator verifies the education record with the person's school or university, and checks his/her driving records, credit rating and bank

account, to see that the account exists and whether "NSF" cheques have been written. References provided by the subject are interviewed. At least one previous employer is interviewed to verify dates of employment and reason for leaving, and to obtain the former employer's opinion about whether the subject would be considered a security risk. In the event that an unfavourable characteristic of the individual is brought to the attention of the investigator, the investigator continues with the inquiries in order to confirm the validity of the unfavourable reference. Finally, the intelligence and security files of the OPP and other major police forces are checked.

These procedures are laid down in a set of guidelines to investigators who make the final recommendation on security clearances. The agency which requested the check to be done is simply told whether or not security clearance has been granted. No reasons are given, and neither are any given to applicants for the position.

The second type of security clearance is for positions which are not considered to be particularly sensitive. The subject also signs a form agreeing that a security clearance check may be done. It involves a criminal record check against RCMP files, for which fingerprints are provided by the individual.

The documents accumulated in the course of security clearance are filed at the Security Branch. It is not the practice of the Branch to update a security clearance, unless requested, and this usually occurs only

when a person moves to a position requiring the high level security check.

No checks are undertaken by the Branch for ministries or agencies other than those mentioned, unless specifically ordered by the Commissioner of the OPP. This is said to happen rarely, as a result of manpower restraints, and the fact that the work involved is so time-consuming.

One aspect of this practice raises a concern for the privacy of candidates. Subjects are not told the reasons for denial of a security clearance. With the high security clearance, there is likely to be on file information about the individual obtained from other people, on the basis of an express or implied promise of confidentiality. The New South Wales Privacy Committee assessed the competing interests in this situation and devised the following solutions:

... since intelligence information is of such a peculiarly sensitive nature, it would be undesirable to forward a copy of the report to the person concerned for verification and comment. We consider that this need not preclude the person from being given reasons for the opinion given in an advance report. 17

In this way, the confidential aspect of an intelligence report is preserved while giving the applicant as full disclosure as possible of the particularly sensitive information. Presumably, investigators take appropriate precautions against reaching a decision on the basis of erroneous information. This should prevent situations arising in which

17 Privacy Committee, The Privacy Aspects of Employment (Sydney, New South Wales: 1977) 14.

legitimate complaints can be made about inaccurate reports leading to the refusal of a clearance. In any case, an investigator who has followed such precautions should have nothing to fear from the revelation that a particular report is inaccurate. In our view, an applicant should be told the reasons for not receiving a security clearance and should have an opportunity to explain any unfavourable information gathered about him/her or to correct wrong information.

With the low security check, we see no difficulty in giving the individual the full results, if requested, since this conviction data is in any case available under the Canadian Human Rights Act from the RCMP. At the same time, those who provided information to the investigator, with the subject's consent, should receive assurance that the confidentiality protects the source of the comments, but not the information itself. The New South Wales Privacy Committee recommended that where a person is being considered for employment and a criminal record or arrest record is revealed, the candidate should be given an opportunity to see the report to verify its accuracy, and to explain the occurrences. The Committee found that in many jurisdictions, criminal histories may be misleading where the disposition is not shown, and an arrest record shows as a criminal record.¹⁸

18 See Privacy Committee, The Privacy Aspects of Employment, op.cit., 14; and U.S. Privacy Protection Study Commission, op.cit., 242-249.

It must be noted that the Branch has never been asked to provide reasons for not granting a clearance, largely because few clearances are in fact turned down.

In sum, a strong argument can be made that where an applicant for a position is not granted a security clearance, s/he shall, on request, be given an opportunity to discuss the reasons for rejection with the investigating officer and to view his/her file, provided that the identities of confidential sources are not revealed.

D. Records Created During
the Course of Employment

Most of the recruitment information collected about the candidate is kept for the purpose of personnel administration, if a decision is made to hire the applicant. Additional information enters the file as the employee's career progresses.

If the candidate is already a civil servant, recruitment information may be placed in a "competition file." These files are held by the Civil Service Commission or the hiring ministry. Responsibility for recruitment to most positions has been delegated to the individual ministries. Most hiring for civil service jobs draws on the already existing civil service. Thus, most employees have competition files in addition to the other data described hereafter.

Once a decision has been made to hire an individual, personal information is collected for several purposes. This information is used for decision-making in respect of the individual employees, in addition to determinations made without reference to specific individuals. These decisions on an individual level include hiring, firing, classification and benefits during the course of employment and upon termination; and on a general level, manpower planning and negotiations about conditions of employment.¹⁹

New employees of the Ontario government may have a variety of forms to fill out for employee benefits purposes. There is a statement to be completed by those who wish to contribute to the Public Service Superannuation Fund. A form must be completed indicating OHIP (Ontario Health Insurance Plan) status. If the employee wishes to be exempt from the employer's OHIP group, additional forms must be completed. The province of Ontario employee group insurance plan allows employees

19 U.S. Privacy Protection Study Commission, op.cit., 226. The Commission describes records examined in its study of employment records:

Employment and personnel records serve a number of purposes. Here the focus is on their use in decision-making about individual applicants, employees, and union members rather than on their use in making decisions about groups of individuals. That is, the Commission's focus on the use of employment and personnel records in deciding whether to hire, fire, replace, transfer, promote, demote, train, discipline, and provide fuller personal benefits, rather than on their use in deciding whether to modify compensation claims, a recruitment policy, or an affirmative action program.

to apply for life insurance, supplementary health and hospital insurance, and long-term income protection insurance through the employer. Forms must be completed in respect of each plan. Health and other personal information may be required, although the most detailed health information collected in this way is held only by the insurance carrier. The information retained by the government indicates beneficiary, marital status, type of insurance coverage, and salary. Claims are administered by the Ministry of Government Services, but no details of the claim are retained in their files. The employee's tax deduction return form (TD-1) is standard to most employers in both the private and public sectors. It indicates tax deductions for which the employee qualifies. This information is returned to the federal Department of Revenue for taxation purposes.

1. Computer-Held Files: IPPEBS

Prior to 1976, employee information for payroll, personnel and employee benefits administration was held in three central computer systems for personnel purposes. At the ministry, this information was merged in the "corporate" file. Between January and October 1976, the centrally held files were converted to the Integrated Pay, Personnel and Employee Benefits System (IPPEBS). As the name indicates, the system involves the integration of three record systems. The purpose of the merger was the reduction of duplication of information common to all three files. The ministries were required to operate on the IPPEBS system by November

1, 1976 with their classified or complement staff. It was optional to the individual ministry to put records for unclassified staff on the system. At the time of writing, only two ministries have no unclassified staff on IPPEBS. However, none has all its unclassified staff on the system. Concurrently with the creation of this central data base for employee records, all manual documentation was placed in the hands of the individual ministries. Ownership of this information rests with the Civil Service Commission under The Public Service Act.²⁰

An IPPEBS advisory committee, composed of selected ministry representatives, makes recommendations with respect to technical and procedural problems from the ministry viewpoint. The central agency coordinates policy. The data base provides a central source of data on every governmental employee on the classified staff for the purposes of issuing paycheques on behalf of Treasury, of administering benefits, and of controlling personnel transactions by the Civil Service Commission. There are "fields" available on the data base which may be used by

20 While information ownership is a notion shunned by many experts, it is used in the context of the Civil Service Commission to designate the extent to which it controls collection, transfer and use of employee information; s. 4 of The Public Service Act, R.S.O 1970, c. 386 as amended, requires the CSC, among other things, to "evaluate and classify each position in the classified service and determine the qualifications therefor"; to "recruit qualified persons ... establish lists of eligibles," and "assign persons to positions in the classified service." The records generated in this connection are hence required to be kept by the CSC. These duties may be delegated to the ministry levels, but a condition of ministry creation and handling of "corporate files" is that they be returned to the CSC upon its request. Such is the nature of CSC ownership of this information.

ministries for functions relating to IPPEBS-type information, but which are not standard across government. For example, a ministry may keep payroll information concerning unclassified staff in the data base.

Shortly after the introduction of IPPEBS, some ministries expressed an initial dissatisfaction with the system. There was a great workload involved in converting personnel records to the automated system. Some objected that centralization of record systems gave the Civil Service Commission access to more information than it had previously; for example, payroll information became available. It was felt that the integrated data base gave the CSC additional and unnecessary access to personally identifiable information. It may be, however, that this concern resulted more from inter-agency rivalry than from an awareness of privacy issues. For the CSC, a major reason for the implementation of IPPEBS was to increase efficiency and completeness of the record-keeping process. The system allows the CSC to perform personnel inventory, budget projects, and other statistical manipulations on the data with greater ease. The overall staff was expected to decrease through the combination of these systems. Whereas previously each ministry required personnel clerks, payroll clerks and employee benefits clerks, now in most ministries IPPEBS clerks fulfill all three functions using the integrated data base.

With the implementation of IPPEBS came a need for additional staff to process the information at the computer installations. Ministries transferred information via government messengers to the Employee Data

Services Branch (EDS) of the Ministry of Government Services in batches, often on a daily basis. The Government Payment Branch needed keypunch operators to enter payroll information on magnetic tape for storage in its computer. Data entry is carried out by the Employee Data Services Branch through on-line terminals to the Queen's Park Computer Centre. Output from the system is provided directly to the Employee Data Services Branch (EDS) through remote printers within the Branch.

The EDS Branch was set up specifically to maintain IPPEBS. Its main functions are to operate, maintain and improve the IPPEBS and attendant computer systems. It is responsible for keypunch, control of data, data entry, modifications to programs and maintenance, and implementation of changes to the system. The Branch is located in the physically secure George Drew building. Through this location, and the frequent changing of passwords needed to access the computer, the security of the data is protected.

It is the individual ministry which is responsible for the accuracy and currency of its own employees' data. Information is submitted at the originating ministry's discretion on forms designed by EDS. These forms reflect the content required by the Civil Service Commission and the Ministry of Treasury, Economics and Intergovernmental Affairs.

Although batches may be sent over as often as daily, updates are not generally performed more frequently than every two weeks, at the same time as bi-weekly paycheques are processed. In addition to the many

different kinds of reports which may be requested as a routine matter from EDS, ministries may request special analyses to be made of their own personnel data. New reports requiring new programs may be obtained, depending on the resources available to the EDS and its assessment of the general utility of the report requested.

A total of 94 data elements concerning an individual may be stored through IPPEBS. The IPPEBS is considered to be simply an information storage system. It does not constitute the official employee record -- the documentary file held by the ministry for whom the individual works -- known as the corporate employee file. As indicated previously, with the introduction of IPPEBS all manual documentation was placed in the hands of each ministry for inclusion in these official files.

The primary use of the IPPEBS data base is payroll. In addition, the data base generates and updates an Employee Service Record report. This report contains on one document information about classifications, transfers from job to job, salaries, benefits, income tax exemptions, Social Insurance Number, sick days, and vacations.

The data base was designed to use the Social Insurance Number as the critical identifier of employees. The employee's Social Insurance Number serves as the file number of the system and is present on nearly all input documents. However, when a user-ministry requests its own output, it may use another identifier. Some unique personal identifier is necessary in using a large data base such as IPPEBS, since

alphabetic names are not totally reliable. In addition, SIN is a requirement for payroll purposes in the determination of income tax and Canada Pension Plan payments, and is therefore a logical identifier to use for personnel records. The secure location of the computer file, the changing of passwords, and strict access rules to the IPPEBS data base are considered by those responsible for the system as sufficient safeguards against abuse.

We were informed that the material found in letters of reference and detailed work and education histories may in future be made part of the computerized data base. This would constitute a "skills inventory" for use in personnel planning. It may be argued that the inclusion of such sensitive data on the file should only be made with the knowledge of the employee. There are difficulties of which the employee should be made aware in adapting such subjective information to a computerized form. The employee should be afforded the opportunity to give informed consent prior to the storage and use of data about him/her and to inspect the record held on the computer to ensure its accuracy.

To our knowledge, the OPP and the Ministry of Transportation and Communications are the only branches of government which presently keep skills inventories for manpower planning purposes. The MTC file includes all classified staff higher than the "Pay Bank 15." The OPP has computerized its manpower inventory system, to help determine postings for its uniformed staff and to identify those with special skills. A considerable amount of biographical data is obtained directly from

the individuals concerned. Factors such as the spouse's home town and children's ages are included in the file, presumably on the theory that these may be relevant to a posting decision.

2. Manual Files

In addition to the computer-held files, there are a number of types of manually-held employee files. Some serve as backup and supplement the computerized information. As a general rule, manual files are held by the individual ministry personnel branches and often at branch locations around the province. For unclassified staff not on IPPEBS, a manual file constitutes the basis for the same payroll and employee benefit transactions performed by IPPEBS for classified staff. Included in the ministry-held personnel file (the "corporate file"), in addition to documents which support IPPEBS data, are performance appraisals, reference letters, education certificates and other correspondence relating to the work history of the individual. At the branch level, this type of file is known as the personnel file. If an employee launches a grievance of some kind, a grievance file may be established and held at the ministry or branch location, or both. A further set of manual files is maintained by the Employee Health Services Branch. If a mandatory referral²¹ for medical examination is made, this information may also be held in a separate file at the ministry and/or branch level. Each of these files is described below in greater detail.

21 See infra, p. 463.

a) The Corporate File

Much of the data collected at the pre-employment and hiring stages is retained in the corporate file. In fact, it would appear that the only material not retained for the corporate file is background material such as letters of reference, useful in the hiring process but not of any particular value thereafter. A sampling of corporate file content reveals the following types of documents:

- . photocopy of birth certificate, proof of citizenship, landed immigrant form, translation of birth certificate
- . Workmen's Compensation Board reports
- . vehicle accident reports (re drivers)
- . staff requisition (requesting permission to hire a person)
- . interview assessments
- . applications for education assistance
- . education and training results
- . life insurance applications
- . credit union payroll deductions
- . fingerprint forms, in the case of OPP and corrections staff
- . appraisal reports
- . grievance documents
- . discipline records.

The Ontario Manual of Administration states that the Civil Service Commission maintains the following information on current employees:

- . Nomination for appointment to probationary staff, Form CS-301

- . Qualification and ancillary clearance, Form CS-301
- . Employment status change, Form CS-3002
- . Special leave of absence, Form CS-66.

Three other forms are retained in addition to these, where the employee leaves the government:

- . Separation notice, Form CS-5
- . Gratuity forms
- . Final employee service record, Form CS-36.

In addition to the corporate file, the personnel branch may maintain local personnel files containing correspondence and notes about the employee in matters which are of significance to the individual's relationship with the ministry. These documents may serve as background to a disciplinary proceeding launched by the ministry. Although a separate file is often kept on employee grievances, the supporting material is sometimes contained in the corporate file. There is a similarly disparate pattern with respect to mandatory referral files concerning employees who have been referred for a medical appraisal under The Public Service Act.²²

22 The Public Service Act, R.S.O. 1970, c. 386 as amended; R.R.O. 1970, Reg. 749 as amended, s. 74.

b) Grievance Files

A grievance is the procedure used to resolve "a complaint or difference" between the employer and employee. The OPSEU Collective Agreement states its purpose thus:

It is the intent of this Agreement to adjust as quickly as possible any complaints or differences between the parties arising from the interpretation, application, administration or alleged contravention of this Agreement, including any question as to whether a matter is arbitrable.

23

A grievance is initiated by the employee and may be resolved by the agreement of the parties, by attempts at reconciliation, or by an arbitration before the Grievance Settlement Board or the Public Service Labour Relations Tribunal.

Typically, the file compiled upon initiation of a grievance contains:

- . an application
- . a statement of grievance
- . correspondence between the Registrar of the Board and the union or employer, giving notice of the time of the hearing, the name(s) or the arbitrator(s), and notice of the preliminary objections, if any
- . notes taken during the hearing.

The Board holds its file for two years, until all possibility of judicial review is exhausted. The file is sent to the Records Centre, after any notes of the evidence given at the proceedings have been deleted.

23 Collective Agreements between Management Board of Cabinet and Ontario Public Service Employees Union respecting working conditions, February 1, 1978 to January 31, 1979, Article 27.1.

The employer ministry may or may not retain its grievance file. Some employers keep nothing after the proceedings; some only retain a note of the outcome; and some keep the whole file, which should be nearly identical to the one at the Grievance Board. The reason given for retaining little or no trace of the grievance is that some employers are sensitive to compiling a negative profile of an employee. Even when the employee prevails in his/her grievance, the mere fact of having filed a grievance may mark the employee as a complainer or a troublemaker, in the eyes of some. Those who keep the whole file believe that more information about an employee leads to better personnel administration.

c) Medical Records

Medical records about Ontario government employees are generated through the Employee Health Services. Two types of medical records are kept; the employee personal record, and administrative records. The employee personal record may include entries in four systems:

- 1) a card in the receptionist's file,
- 2) chronological recall index,
- 3) alphabetical listing of employees,
- 4) terminal shelf digit system, which indicates the physical location of the file.

Administrative records are also maintained by the Health Services Centre for internal purposes. In addition to record maintenance in the

Health Services office, some medical information may be stored by the employer-ministry.

1) General Health Records

Some medical records are created in the hiring process. The Manual of Administration authorizes compulsory tuberculosis screening for employment. The results of these screenings are interpreted by the Health Service, and an opinion as to the suitability of the candidate is communicated to the personnel officer at the hiring ministry. This is the only medical information which is returned to the personnel officer as a matter of course.

In addition to the chest x-ray, an employee personal file will typically contain records pertaining to general medical examination, vision, recall for immunization, and, less frequently, psychological problems. General medical examinations are routinely conducted for the Ontario Provincial Police, the Ontario Government Protective Service, and three job categories within the Ministry of Transportation and Communications: driver examiners, vehicle inspectors, and highway carrier examiners. The Ministry of Labour requires comprehensive physical examinations every two months for all operational employees. Compulsory examinations are required by The Occupational Health and Safety Act²⁴ for employees

24 The Occupational Health and Safety Act, S.O. 1978, c. 83. (Came into force October 1, 1979.)

handling toxic substances such as lead or mercury, or working under hazardous conditions such as high air pressure. Any ministry may request a pre-employment physical on the authority of the deputy minister.

The primary source of the information in these files is the employee. The other sources of information are the employee's attending physician and any treatment records. An employee may refuse any of the examinations listed above, and the Health Services Branch may advise the appropriate personnel officer of such a refusal. As with all information required in the pre-employment process, however, a refusal to give information may result in a refusal to hire.

A written authorization from the employee is considered necessary by the Service for any transfer of medical information. The information returned to personnel departments as a result of pre-employment examination is the certificate of the examining physician, which simply indicates that the named person has been examined by a Health Service physician and has been either granted or denied a recommendation to be hired as permanent or temporary staff. Re-examination may be recommended, and there is a small space for remarks. The form should reveal no confidential medical data, only a conclusion. The relationship between a medical officer at the Employee Health Services and an employee is identical to a private doctor-patient relationship, and the confidentiality of this relationship is prescribed by The Health

Disciplines Act,²⁵ which enshrines professional ethics in statutory form.

The pre-employment report and other medical reports such as those resulting from mandatory referrals is stored in the employee's corporate file, and in some ministries, at the employee's local office. In one instance we found that medical reports are kept separately. This is in the case of the 8,000 employees of the Ministry of Health, who are located at the psychiatric hospitals. There, the Health Services office keeps all employee medical information in a separate filing system.

2) Direct Services

Direct services to employees include emergency care, general treatment, advice, and rest. Employee visits to the Health Services Centre to obtain these services are recorded in the administrative record, which is held in the form of a ledger to which entries are made for each day. The disposition of such a consultation may be reported to personnel managers, but only as it affects attendance, confirming that a person was sick.

25 O/Reg. 577/75, s. 26(21).

3) Mandatory Referral

In circumstances of repeated absenteeism or inability to perform adequately, an employee may be referred for medical assessment during employment. Known as a "mandatory referral," this is of particular concern where alcohol or drug abuse is suspected. The authority for such examination is in The Public Service Act²⁶ or the Collective Agreement Respecting Employee Benefits, for employees covered by that Agreement.²⁷ Originally, the purpose of the legislative provision was to assure that sick pay provisions were not abused. If an employee was absent for more than five days, a doctor's certificate was required in order that pay not be interrupted. In 1963, the legislation was amended to allow medical examination to be ordered, and in 1966, it was announced that this examination referral power would be used as part of the government's alcoholism program.²⁸

The Manual of Administration includes the following as a policy statement, indicating that participation in the government program on alcoholism may be a condition of employment:

26 R.R.O. 1970, Reg. 749 as amended, s. 74.

27 Collective Agreements between Management Board of Cabinet and Ontario Public Service Employees Union Respecting Employee Benefits, October 1, 1977 to September 30, 1978, Articles 13.9, 13.10.

28 O/Reg. 173/63.

... assistance will be given to the employee in order to return to efficient job performance; however, the employee will be required to accept certain conditions related to the program of rehabilitation which have been determined for him ... Removal from employment must be considered, if it is established that medical treatment or other measures have failed, or if the employee refuses to co-operate. 29

The Regulation states in general terms that

where for reasons of health an employee is frequently absent or unable to perform his duties, his deputy minister may require him to submit to a medical examination at the expense of the ministry. 30

The employee may be required to undergo further medical examination as the Civil Service Commission sees fit. The cost of these examinations is paid by the Commission.

The Employee Health Service reports that last year, of the 248 mandatory referrals for examination, 48 were alcohol-related matters.³¹ Most of the others arose from circumstances where malingering was suspected. In a few instances, a psychological problem may be suspected as the root cause of poor work performance or attendance problems. Whatever the motive for the referral, a form entitled "Authorization and Release" must be signed by the employee. It is reproduced on the following page.

29 Ontario Manual of Administration, Vol. 2, 6-60-1, June 1, 1976.

30 R.R.O. 1970, Reg. 749 as amended, s. 74(3).

31 Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario, Transcripts of Investigative Hearings, Vol. 92 (March 13, 1979) 50. The total of examinations conducted by the Service is nearly 70,000. While the total of mandatory referrals may be somewhat higher than 248, the very small number of referrals for alcohol-related problems is much lower than anticipated when the program was introduced.

I,
am fully aware that I have been referred under the authority
described on page one of this release and that the professional
staff of the Employee Health Services Branch is obliged to
submit a report to the referring Officer in my Ministry.

I understand that the report will contain a diagnosis of my
condition including pertinent background information where
necessary, a statement of my condition at present my ability
or inability to continue to work with or without modification
of my present job.

In signing this Authorization and Release, I certify that I
have read this document and that I understand its contents.
Further, I authorize the staff of the Employee Health Services
Branch to perform said examination, to prepare and submit a
report of my condition and to make appropriate recommendations
concerning me and my job to my employing Ministry.

.....
WITNESS

.....
SIGNATURE

.....
DATE

The use of the word "authorization" on this form may be thought to be somewhat misleading. As the first paragraph states, the report which the form purports to authorize must be rendered by the Employee Health Services Branch to the referring officer as a matter of statutory obligation, although it may be argued that only certificates after five days absence are required by statute.³² The use of this authorization and release form results, no doubt, from the obligations imposed by law on medical professionals to preserve confidentiality of health information about patients, unless authorized in writing to release the information. An employee's refusal to sign the "Authorization and Release" would result in the Health Service refusing to conduct the examination. The refusal to sign the authorization is therefore considered to be a refusal to take the medical examination. This, in turn, could be considered grounds for a dismissal; however, we know of no cases in which this has occurred.

In effect, then, while the form must be seen as an authorization for the purposes of The Health Disciplines Act, an employee whose examination is duly required and who wishes to remain employed does not have any real choice in the matter.

32 Supra, notes 26 and 27. In the course of the Royal Commission hearings referred to at note 31, Commissioner Justice Horace Krever stated that it is a matter of necessary implication, in the statutory language, that the Health Service communicate its findings to the referring ministry. (Transcripts, op.cit., 72.)

The statutory provisions now authorize the government program on alcoholism. The program is set out in detail by the Ontario Manual of Administration in the section of the manual concerning conditions of employment.³³

No doubt, the detection of alcoholism and its recognition as an illness may be in the employee's interest. There is reason for concern, however, that the records of the sensitive information generated by this program are not given the same confidential status as the other medical records generated as a matter of course in the employee relationship.

An employee may initiate a rehabilitation program on his/her own, in which case confidentiality will be maintained about the employee's seeking out the program, and his/her progress through it. If a ministry official initiates the referral, however, a warning letter is sent to the employee stating the performance problem perceived by the employer to be rooted in alcohol use. A copy of the letter stays in the employee's corporate file. After the medical examination, a report on the prospects of improved performance and diagnosis is sent back to the personnel department and is placed in the corporate file. The diagnostic report may confirm the problem, and may contain an outline of a treatment program. In this way, sensitive medical data is mixed with other personnel data on file.

33 Ontario Manual of Administration, Vol. 2, 6-60-1 to 5, June 1, 1976.

The confidentiality problem arising in the process results from the fact that sensitive medical information is transferred to persons who are not health care providers, but who make decisions about the individual's employment. These records are stored together with the more routine documentation in the corporate file with the consequent possibility of access by supervisors and co-workers. The legitimacy of the employer's requirement that an employee submit to a medical examination stems from a concern for the employee's health and from a need to determine whether "normal work performance and productivity"³⁴ will be restored. It does not appear necessary, in meeting this need for information or advice, to release sensitive medical data to a person who is not qualified to analyze it, and whose working relationship with the individual may render the possession of sensitive personal data in his/her hands an undue invasion of privacy. A strong argument can be made that where a medical examination is compelled in order to determine whether unsatisfactory job performance may be remedied, only an assessment of the employee's work capacity should go to the employer from the physician. No medical information should be returned to the referring deputy minister or supervisor. In order to preserve the confidentiality of such material, the Health Services Branch could restrict its communication to the referring official to an opinion of present and future work capacities.

34 Ibid., 6-60-1.

The Privacy Committee in New South Wales has noted that there is a "risk to the traditional confidential relationship between patient and doctor" when medical services are available to the individual at work, "unless great care is taken to insulate that relationship from the work-related responsibilities of the medical staff."³⁵ For the majority of medical records generated in the employment relations of the Ontario government, this insulation appears to be inadequate. The Employee Health Services maintains its record-keeping system independent of personnel services. The staff at the Service exhibits a high consciousness of and solicitude for the confidentiality of health records. In most cases, the only record of medical information in the employee corporate file is the tuberculosis report. In the case of mandatory referrals to the alcoholism program, however, there is a comingling of medical and work records which are accessible to personnel officers and other co-workers of the record subject. This is the situation against which the New South Wales Committee warns. We echo its sentiments.

4) Record Storage and Security

All records generated by the Health Services Centre are maintained manually. This is also true of health records maintained in the Employee Health Services Branch offices in Toronto and the one at Sudbury. At the

35 Privacy Committee, op.cit., 39.

Queen's Park location, the file cabinets containing medical information are kept locked, although the treatment cards are not locked up. The Centre is constantly under supervision. Though security measures at other offices are not uniform, there appear to have been no complaints or problems perceived in relation either to physical security or methods of collecting data.

The medical files are retained at the Centre until an employee leaves the government. His/her records are then sent to the Cooksville Record Centre, and held for another ten years. Of the administrative records generated by the Centre, the daily record and the summary of daily records, which contains no personally identifiable material, are kept for two years.

E. Access to Employee Records

As we have indicated in our general discussion, many observers believe that a key protection of informational privacy is found in obtaining access to one's own record. Access as a concept may be considered to be limited to simply viewing the record, or may include the taking of copies. Further, many feel that it is essential to provide the record subject with a means for challenging the accuracy and completeness of the record so as to provide an opportunity to ensure that the individual is not prejudiced by the use or transfer of erroneous information.

In addition to subject access, contemporary approaches to informational privacy focus on the need to control access to records by others than those to whom the data was initially provided. The commonly employed criteria for transfers of confidential material are "need to know," or uses which are "consistent" with the purpose for which the information was collected.³⁶ To distinguish third party access from subject access, and to stress the record-holder's responsibility for circulation of the record, we will refer to third party access as transfers of the record.

1. Personnel Records

a) Subject Access

The government of Ontario has no uniform policy governing the employee's access to his/her own record. A survey of personnel record-holders, conducted for this study, indicates a range of response to the questions

36 The American Privacy Act, 1974 allows disclosure of personal records among federal agency employees and officers where they have "a need for the record in the performance of their duties" (5 U.S.C. s. 552a(b)(1)). The Canadian Human Rights Act allows transfer of a record among agencies without consent from the data subject where the recipient purpose "is consistent with the use for which [the record] was compiled," in the minister's opinion (s. 49, s. 52(2)).

"Does the employee have access? Under what circumstances? What if the employee challenges the record?"

Of 21 ministries, only two gave an unqualified positive response to the question, "Can an individual have access to his or her file?" Only two gave an unqualified negative response. The remaining 17 require some supervising presence while the employee examines the file. Some indicated that this was as a security measure; others stated that the personnel officer would assist the employee in understanding the file. One ministry restricts employee access to situations constituting a "valid reason." Even so, there is no "direct" access for that ministry's employees. Presumably this means a supervisory officer would review the file with the employee. In another ministry there is access only when a grievance is pending.

Two ministries described a Minute of Understanding to which they have agreed.³⁷ It provides that an "employee is to be made aware of any written commendation, reprimand or adverse report," and sets out the means by which such a report might be challenged. This is similar to agreements maintained by some Boards of Education in Ontario, in respect of their employees. It reflects an important principle in fair information practices which has been recommended in other jurisdictions, and is being implemented voluntarily by some private sector employers.

37 Ministry of Correctional Services, November 13, 1973; Ministry of Natural Resources, July 8, 1975.

Where appraisals are filed and may be used in decision-making processes, the employee has an obvious interest in being given the opportunity to know the contents, and correct inaccuracies. We believe this interest to be worthy of protection.

The majority of ministries responded negatively to the question, "Would any parts of an employee's file not be open to access by the individual?" Three stated that medical information may be kept from the employee's inspection, and three would exclude confidential references or appraisal reports.

There appears to be no policy in place governing employee access to one's own IPPEBS file. Policy has been set out for access by a variety of third parties. The Employee Data Service expects subject access requests for this material to be handled by the appropriate ministry, which has full access to its data processed by EDS.

b) Transfers

1) Access by the Civil Service Commission

The Civil Service Commission (CSC) owns all corporate files, although as described above, it is the individual ministry which holds all of

them, since the introduction of IPPEBS.³⁸ Under section 25(1) of The Public Service Act, the CSC has a right to access these files, and upon its request, the files must be produced within seven days. The CSC may obtain personally identifiable data, or summarized material. The CSC also has access to all common IPPEBS data, which is not surprising in the light of its "ownership" of some of the supporting documents. Although it does not "own" pay data, it claims access to it.

2) Access by the Employee Data Services Branch

In its role as manager of the IPPEBS System, the Employee Data Services Branch has access to any IPPEBS data required to operate the system.

3) Access Within Ministries

As a general rule, the senior staff in each ministry has access to files. Deputy ministers, directors and assistant directors most often fall into

38 While the term "ownership" is widely considered inappropriate in relation to information, the Civil Service Commission exerts a claim over corporate employee files which is described as "ownership." As the CSC has responsibility for all appointments to probationary staff, and for recommendation and certification for appointment to regular staff, it must have the supporting documentation. However, as a practical matter, this responsibility for file handling is delegated to deputy ministers. They may maintain the files at their decentralized locations, but must send them back to the CSC upon request. This policy will soon be incorporated in the Manual of Administration. This relationship is summarized in the term "ownership."

the category of those employees needing no clearance to view files. Further, personnel branch staff have virtually unlimited access to files. Prior to the introduction of IPPEBS, the clerks working with these files were exposed to less information about any particular employee. One clerk would deal with employee benefit files, another with payroll files, and another with personnel files. No one clerk would as a routine matter be able to obtain a global picture of the employee. Now, with the reduced ministry-level staff resulting from the IPPEBS system, there is a fundamental change in who has access to what in the routine execution of duties. One clerk may now handle all three aspects of the file in respect of an individual employee. Because of this, at least one ministry has refused to amalgamate all these duties, and has separated clerical operations for payroll and benefits transactions from personnel matters.

The adoption of clear written policies on these matters appears to be unusual. To our knowledge, the Ministries of Industry and Tourism, Housing, Natural Resources, Environment, Education, Solicitor General, and Correctional Services are the only ministries which have formulated written rules concerning third party access to personnel files. Other ministries have informed us that although their policy is unwritten, it is known to staff; still others rely on the Manual of Administration, Volume II at 13-10-1. It merely states that "Central files on employees may be referenced upon the authorization of the Chairman of the Civil Service Commission or his authorized official." The Ministry of Community and Social Services responded to our questionnaire that it

had no written policy on third party access, although a memorandum is in circulation dated December 12, 1977 concerning "information and security on personnel matters."

The Ministry of Education has expressed its arrangement in this way:

Personnel data of all kinds including salary, classification, personal status is available only to the individual employee, his/her supervisor and succeeding supervisors in that organizational unit.

For example:

- i) an employee may review the contents of his/her own file in the presence of a Personnel Administrator.
- ii) a Branch Director may obtain any information on employees within his branch, but no information on employees in another branch without the permission of the Personnel Director.
- iii) an Assistant Deputy Minister may obtain information on any employee in his Division, but not information on an employee of another Division without the permission of the Personnel Director.

39

4) Access by Other Government Agencies

In addition to requests from within the ministry, there may be requests for personnel information made from one ministry to another. These are treated differently from requests within the same ministry, and are distinct from general public inquiries. Most third party inquiries of

personnel departments for employee information are in connection with transferred personnel. The Ministry of Correctional Services states that access to file information can only be had for the purpose of conducting the day-to-day business of the employer; that is, the Ministry. Apparently, much of the exchange of information is done by telephone, but approval for direct access to the file must be given by the director of personnel.

5) Access by the Public

Personnel information requests emanate from persons and agencies outside government. Common requestors are credit bureaus, estranged spouses or their lawyers, police, and new or prospective employers. It must be stressed that although these are the common sources of requests, all of our interviewees made the point that inquiries of this kind are infrequent. The general policy seems to be that staff only "confirm" information unless there is a written request or consent by the employee. Thus if someone telephones and asks whether a certain employee lives at 50 Front Street and earns \$15,700 annually, the personnel officer may confirm or deny it, even though the employee may have no knowledge of the inquiry and may not have consented to such disclosures. No "new" information, however, is offered in response to such inquiries.

Records may be subpoenaed in connection with legal actions. This most commonly arises in the context of marital disputes.

6) Access by the Police

The memorandum describing access procedures within the Ministry of Community and Social Services⁴⁰ indicates that police may have access in what appears to be an unlimited fashion. It is described thus:

Police access is provided but only on a personal basis, with the officer showing his/her identification and reason for review. Normally a personnel officer is present during the review.

It is interesting to note that when interviewed, the personnel director for this ministry indicated that there was no policy for third party access. If policies of the above kind are common among ministries, one may assume that the police have relatively free access to personnel files, but that access for other third parties is discretionary.

The question of police access, in the absence of a subpoena or search warrant, is a source of concern. For many it is the investigative activities of the police that represent the greatest threat to their privacy. Carte blanche access is simply not acceptable. There may be

40 Ministry of Community and Social Services, Memorandum concerning Information and Security on Personnel Matters, December 12, 1977.

cases where the police should be given access to personnel records. There may indeed be cases where this access should be achieved without data subject knowledge. On its face, however, this practice is clearly an invasion of individual privacy, and should be regulated at least by policies clearly stated.

c) Union Access

With the exception of management level employees and those specifically excluded from the collective bargaining process by The Crown Employees Collective Bargaining Act,⁴¹ government employees are unionized, primarily within the Ontario Public service Employees Union (OPSEU). In order to fulfil its mandate as bargaining agent, the union may need information about employee members held in the employer's files. Access currently provided under the terms of a letter appended to the OPSEU collective agreements is restricted to "directory" information, i.e., employee name and position. This information is made available only in respect of dues-paying members, although the union is required to represent all those in the bargaining unit.

41 S.O. 1972, c. 67. Section 1(g) of the Act excludes a variety of Crown employees, including the Ontario Provincial Police, employees of community colleges, members of self-governing professions, persons "engaged and employed outside Ontario," and persons employed in the office of the Provincial Auditor.

Union access to information is not mentioned in the agreements concerning Ontario Housing employees within the Canadian Union of Public Employees (CUPE) Local 1750.

2. Grievance Files

Fairness demands that each party to a grievance know the case it must meet. The OPSEU Collective Agreement⁴² states that

The employer upon written request either by the employee or by the Union shall make available all information and provide copies of all documents which are relevant to the [classification] grievance or may be used by the employer in the presentation of the case before the Grievance Settlement Board.

The article refers only to classification grievances. For all other types of grievance, it is the policy and practice of the Board to assure that both parties and the Board have advance notice of material to be used. This practice is authorized for the employer, but not made mandatory, by the Manual of Administration. The Board takes the responsibility of sending material to both parties, and in its reasons for decision in a number of cases the Board has made clear its position of requiring disclosure before an arbitration may proceed. The Board is to be commended for its strong stand in this matter. We would

42 Collective Agreements between Management Board of Cabinet and Ontario Public Service Employees Union, governing working conditions, February 1, 1978 to January 31, 1979, Article 5.1.3.

recommend, however, that access be guaranteed by statute for all grievances. This would avoid the present discrepancy between collective agreements governing the public service. For example, while OPSEU's agreement contains the provisions referred to above, the agreement with CUPE Local 1750 does not include anything similar. Access in all grievance situations should be available from the outset, and not merely at the advanced stage of proceedings before the Board. It is likely that if full disclosure was granted at the outset, more grievances could be resolved at the earlier, less formal stages of grievance resolution, as set out in agreements.

3. Medical Records

There are no formal procedures in place for subject or third party access to employee health records, nor for their correction at the instigation of an employee. To our knowledge there have been no requests for access or correction, but should such requests be made, they would be handled as in any private doctor-patient relationship. At the ministry level, as we have noted, some would withhold medical records from the record subject, although other types of records would be available.

CHAPTER XI

HEALTH

A. Introduction

The original terms of reference of our study directed us to examine personal record-keeping practices and record access with respect to medical health records. However, by the time research on this project commenced, the Royal Commission of Inquiry into the Confidentiality of Health Records, under Mr. Justice Krever, had been established and had already begun an extensive examination of this topic -- involving interviews with hospital officials, physicians, health record users in both the public and private sectors, and health insurers, in addition to holding public hearings and investigations into reported abuses of confidentiality. We felt, therefore, that any field research on our part would duplicate what was already being accomplished by the staff of that Commission. In addition, two studies undertaken for this Commission involved medical records -- one on research uses of microdata¹ and another on the Workmen's Compensation Board.²

1 Flaherty, D.H., Research and Statistical Uses of Ontario Government Personal Data (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 5, 1979).

2 Ison, T.G., Information Access and the Workmen's Compensation Board (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 4, 1979).

Our approach, therefore, in this chapter is to provide a brief outline of the main issues surrounding the confidentiality of medical records, a description of existing legislation affecting medical records and a discussion of possible access rights to medical records. Finally, we examine in some detail the issue of a unique personal identifier or "health care number," which has been proposed for Ontario, and its implications for privacy and confidentiality.

For our study, we have drawn on previous studies of medical records both in Canada and the United States, and on briefs by individuals and organizations to this Commission and to the Krever Commission. We are particularly grateful to Mr. Justice Krever and his staff for their assistance.

B. Confidentiality of Health Records

In order to receive proper medical care and attention, it is often necessary for people to reveal the most intimate details of their bodily and mental functions, personal habits and close relations with others to health care practitioners. If we refer, for a moment, to Charles Fried's explanation of privacy as "a rational context for a number of our most significant ends, such as love, trust, respect and self-respect,"³

3 Fried, Charles, "Privacy, A Rational Context," in An Anatomy of Values (Cambridge, Mass.: Harvard University Press, 1970) 138.

it is easy to see why the information typically shared with a physician is regarded as being so intimate and sensitive. It touches the very centres of knowledge about ourselves, and is therefore given only to those whom we trust, respect and who we believe will treat us respectfully in return.

The strong tradition of professional ethics on the part of health care practitioners, therefore, results in a general absence of concerns over the loss of personal privacy, which by the very process of ministering to the sick is stripped away. It does involve concerns, however, with respect to "informational privacy," or confidentiality of the information which becomes the patient's medical record.

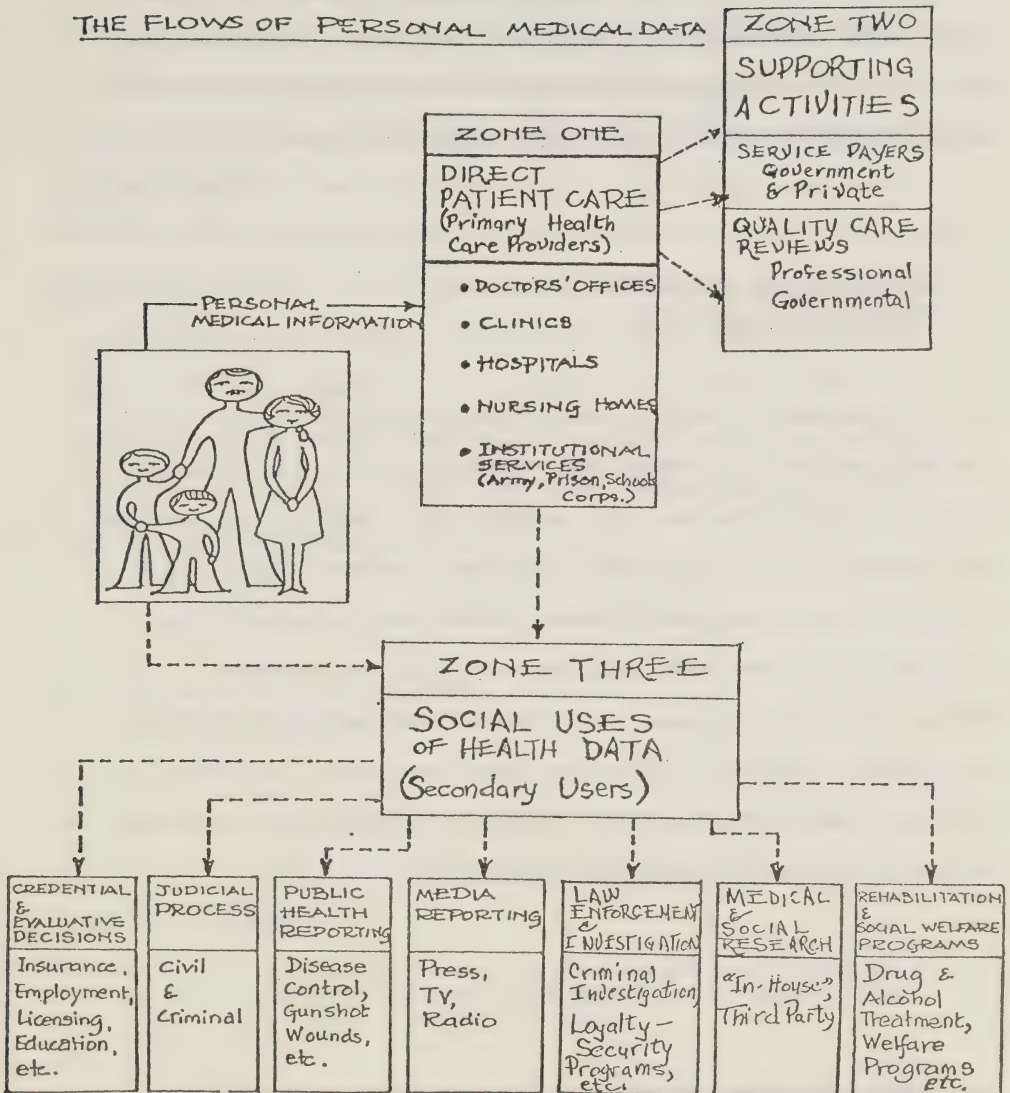
The major privacy issues in the health field have evolved because of several factors:

- a) Increasing specialization and complexity in health services administration;
- b) Increasing reliance on computer technology;
- c) Extensive government involvement in medical record-keeping;
- d) Increasing use of medical records by non-medical organizations, such as insurance companies, employers and the social services.

The sharing of information by a patient with his/her physician was once on a one-to-one basis. Now, however, sharing and transfer of a patient's information necessarily involves a much larger number of people, who may or may not be governed by the same code of ethics as the original physician.

TABLE XI.1

THE FLOWS OF PERSONAL MEDICAL DATA



Source: Westin, Alan F., Computers, Health Records and Citizen Rights (Washington, D.C.: Department of Commerce, National Bureau of Standards, Institute for Computer Science and Technology, 1976) 10.

Gatherers and users of medical information can be broken down into three categories, as shown in Table 1: the primary health care area (physicians, hospitals, etc.), supporting activities (health insurers, etc.), and non-medical users (insurance companies, employers, etc.).⁴ We will briefly discuss each of these categories in turn.

1. Medical Records in the
Primary Health Care Area

A U.S. Department of Commerce study of medical data indicates that in the early part of this century, 85% of medical services were provided directly by physicians, who often worked alone. Records about patients were therefore held by individual physicians, and much of the most sensitive data was retained by memory rather than in document form. At present, it is estimated that less than 5% of the providers of medical care are physicians. Three factors have influenced the wider dissemination of patient information within the medical community: the increasing number of patients per physician, increasing specialization and increasing use of para-medical personnel.

4 These categories, as well as a large portion of the following discussion, are drawn from Westin, Alan F., Computers, Health Records and Citizen Rights (Washington, D.C.: U.S. Department of Commerce, National Bureau of Standards, Institute for Computer Science and Technology, 1976) 9-10 and Chapters 1, 2 and 3.

Although information is more widely disseminated than ever before, the basic trust between patients and their physicians, specialists, nurses and other individuals in the treatment process is still important. To receive the proper care, it is obviously to a patient's advantage to be honest and straightforward in replies to intimate questions. It is also accepted in the highly specialized health care system we have developed, that medical information must be passed from one health care provider to another. For example, we do not question the need for the single medical hospital file to be available to all the health care providers directly involved with a patient's case. Health care recipients also generally recognize the need for health care providers to access and refer to a patient's previous medical history, which is often not available directly from the patient.

a) The Need for Confidentiality
in the Primary Health Care Area

The doctrine of confidentiality has been referred to as the cornerstone of the doctor-patient relationship. This doctrine has its historic roots in the Hippocratic Oath:

Whatsoever I shall see or hear in my intercourse with men, if it be what should not be published abroad, I will not divulge, holding such things to be holy secrets.

This confidentiality is essential because of the sensitivity of information in a medical record, which may contain more intimate details

about an individual than any other single record. In addition to the inherent abuse of patient privacy through disclosure, relating these details to others could result in third parties using and making decisions based on information which the individual neither communicated nor wished to be made known to those parties.

The medical record itself is sensitive over and above the actual medical diagnosis and treatment:

Good medical records contain nuances and impressions, gossip and scuttlebutt; all these notes help a doctor to form a final opinion of the patient, body and soul. 5

Thus, there is potential harm to an individual not only as a result of third parties becoming aware of his/her medical problems or diagnoses, but also because additional information, noted and recorded by the health care practitioner, may be construed by the third party as medical "facts" when they are in effect only observations, not diagnoses.

Despite these potential harms, absolute confidentiality can no longer be pledged. A sharp divergence from the Hippocratic Oath can be seen in the current Code of Ethics of the Canadian Medical Association, which states:

5 Morley, T.P., M.P., F.R.S.C. (C), Professor and Chairman, Division of Neurosurgery, University of Toronto, Brief to the Royal Commission of Inquiry into the Confidentiality of Health Records (Brief #83, April 21, 1978) 1.

An ethical physician will ... keep in confidence information derived from his patient, or from a colleague regarding a patient, and divulge it only with the permission of the patient except when the law requires him to do so.

6

The extent to which confidentiality must be a continuing concern to physicians, hospitals and clinics in the primary health care area is demonstrated by figures provided by a U.S. hospital medical record department to the Privacy Protection Study Commission: 37% of requests for patient information came from other physicians, 34% came from health service payers; 8% came in the form of subpoenas; and 21% came from other hospitals, attorneys and miscellaneous sources.⁷

b) Results of the Erosion of
Doctor-Patient Confidentiality

The abuse (or potential abuse) of information recorded by the health care practitioners can have serious consequences, not only in the negative impact upon the individual record subject, but also in a loss to society as a whole if medical record-keeping practices change. For a specific example:

6 Canadian Medical Association, Code of Ethics, "Patient's Rights" (Toronto: General Council of the Canadian Medical Association, June, 1975).

7 U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society (Washington, D.C.: USGPO, July, 1977) 280.

In recent years the patient records physicians keep in their offices have become subject to subpoena. This, together with the trend toward greater availability of patient charts in hospitals has brought about a change in record-keeping practices among some physicians. Records once contained the most candid comments to enable the physician to recall, months or years later, the precise circumstances relating to a patient. The fear of such comments being read aloud in a court of law has caused many doctors to refrain from including in medical records statements which might be embarrassing under such circumstances, even though they may be extremely helpful in the care of the patient.

8

Thus, a possible reduction in the quality of health care provided to an individual, due to the incompleteness of the medical records kept by physicians, may be directly related to the inability to assure confidentiality.

A lack of confidentiality may also affect the degree to which patients fully disclose important details about their health to medical practitioners. If patients fail to fully reveal medical information to their physicians because of a lack of trust that the information will be kept confidential, the benefits they receive from health care may be negatively affected.

c) Confidentiality and Subject Access

Growing patient concern about the uses made of medical information may also be based on a general ignorance of what is contained in the medical record. Most patients have never been able to see their medical records and assure themselves that information contained therein is correct. Although many statutes stipulate that the record subject give consent before the record is shared with others, a signature does not constitute informed consent when the patient has not seen what will be disclosed.

There is no legislative provision in federal Canadian or Ontario law giving the right of full access to a patient (except in the process of litigation or tribunal hearings). In the absence of statutory obligations to allow patients to see their records, Ontario medical professionals have granted subject access only on a discretionary basis and in unusual circumstances. Under the regulations of The Public Hospitals Act, for example, the executive officer of a hospital board has the discretionary authority to grant access to patient records,⁹ but that authority is rarely used to provide access to patients themselves. The reason given for not encouraging more open subject access is usually that patients viewing their record may be harmed psychologically or emotionally, a position supported by the Ontario Medical Association in a brief to

9 R.R.O. 1970, 729/48(5) (c) (e).

the Commission on Freedom of Information and Individual Privacy.¹⁰

The Ontario Medical Association and the Ontario Hospital Association have produced a joint paper clarifying their position regarding rights of access. Although the paper states as a general principle that "a patient has a right to information about his or her health care," and that a patient may expect to receive information from the hospital medical record, nowhere does it recommend that patients as a matter of course be allowed to personally examine, question or correct records held either by hospitals or by their personal physicians. A caution against complete subject access is stated in the form of a principle:

It is essential that undue access to such information does not inhibit the complete recording of adequate and valuable data necessary for the continuing care of the patient.

In an accompanying letter, explaining the guidelines to Chief Executive Officers of hospitals, the OHA suggests a further barrier to complete subject access by approving the notion that attending physicians have

10 Ontario Medical Association, op.cit., 3. "We believe patients have a right of access to certain information on their hospital charts, but not unlimited or uninformed access. Patients who are unaware of the content of their records and unsure of their ability psychologically to handle the information need the protection of the professionals who produce the records and can assess the hazard to the best interests of the patient in providing access. (emphasis added) Discretionary denial of access to medical records is supported by Treasury Board Regulation No. 24 under the Canadian Human Rights Act, Part IV (s. 62(1)(d)), which states: "Where a medical practitioner expresses the opinion that the examination of a medical record, whether or not a psychological report, by the individual whom it concerns, may be contrary to the best interests of that individual, the government institution shall inform the individual that the record or report is not available for his examination."

the discretion to withhold some medical information if there is reason to believe that it

may have a significantly adverse psychological effect on the patient, or that the patient will be unable to deal with the information in a rational or responsible manner.

Where access to medical information is granted, the paper directs physicians to provide a "fair interpretation," explaining the uses and contexts of medical terminology to the record subject.¹¹

It is interesting to note comments regarding the effects of patient access made to the Krever Commission staff by administrators at the St. Elizabeth Psychiatric Hospital in Washington, D.C.¹² Because it is a federal institution, St. Elizabeth's adheres to the requirements of the U.S. Privacy Act, which mandates individual access. As a general policy, direct access rather than access through an intermediary physician has been provided to the requesting patient. Although it created a temporary administrative workload, patient access had been permitted for almost 18 months (at the time of the Krever Commission visit) with no reported adverse patient effects. Indeed, certain

- 11 Ontario Hospital Association and Ontario Medical Association, Guidance Regarding the Expectations and Responsibilities of Individuals and Institutions in Health Care with Respect to the Release of Information from Hospital Medical Records (Toronto, November, 1978) 1-4, and accompanying letter from R. Alan Hay, Executive Director, Ontario Hospital Association to the Hon. Mr. Justice Horace Krever, January 10, 1979.
- 12 Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario, Research Staff, Memorandum re Visit to St. Elizabeth's Hospital (Toronto, November 8, 1978).

benefits emerged through greater openness and trust between medical staff and patients. A predicted disadvantage of subject access had been that subjective information useful to a medical diagnosis would be kept in an "unofficial" record, unavailable to either the patient or other specialists and medical staff dealing with the patient. However, those interviewed at St. Elizabeth's stated that treatment personnel were "not keeping two sets of notes" to avoid subject access provisions.

2. Supporting Activities:
Medical Records used by Health Care
Service Payers and Health Care Reviewers

The primary third party medical service payer in Ontario is the Ontario Health Insurance Plan. OHIP is a Ministry of Health operated insurance company which pays registered health care providers for services provided to more than eight million individuals covered by the plan. As the amount of payment depends on the type of service rendered, it is essential that diagnostic and procedural information about individual subscribers be given by hospitals and doctors to OHIP for billing purposes. In addition, OHIP also maintains this information to conduct periodic audits and reviews of health care billings, and to compile profiles of service users and providers in order to detect and investigate abuses of the plan. The Minister of Health and the Registrar for Health Insurance have investigatory powers under The

Health Insurance Registration Board Act to inspect the medical and financial performance of health care practitioners and facilities in the context of provision of insured services.¹³ During such audits and inspections, personal medical records provided by physicians and hospitals are used by Ministry and OHIP staff.

Much of the information retained by OHIP and the Ministry of Health is computerized. The Ministry is one of the major users of computers in the Ontario government. In addition to the OHIP subscriber file, the Ministry holds computerized records of, for example, victims of contagious diseases and persons eligible for drug benefits, in its role as monitor of the state of health and health care in the province.

Requirements for confidentiality of OHIP records, including many exemptions to requirements, are set down in The Health Services Insurance Act.¹⁴ As far as individual access to OHIP records is concerned, we were informed that such requests would normally be granted, although officials retain the discretion to withhold the record if a medical diagnosis could upset a patient. In fact, OHIP has received few requests from people wishing to see their record. It is our understanding that doctors often couch diagnostic descriptions on OHIP billing documents in such a way as to minimize disclosure of information

13 The Health Insurance Registration Board Act R.S.O. 1970, c. 199, s. 6.

14 The Health Services Insurance Act R.S.O. 1970, c. 200, s. 23.

which may seriously infringe upon a patient's privacy, or which may prove upsetting to the person concerned. In the belief that users should be more aware of the cost of services provided by public agencies, OHIP has, on request, provided statements to subscribers of medical services received and paid for by OHIP.¹⁵ However, in cases where the head of a family is the registered subscriber to OHIP, this practice may infringe upon the privacy of individual family members, who seek independent medical advice. (This problem could perhaps be overcome by introducing OHIP numbers for all OHIP users.)

3. Non-Medical Users of Health Information

The marked increase in sharing patient information within the medical community has been accompanied by an equivalent growth in patient information sharing with non-medical users. Although medical record-keeping practices in the private sector are not the focus of this study, their significance to the privacy of Ontario citizens and their relationship to government record-keeping practices cannot be overlooked. Three potential non-medical recipients of health records are insurance companies, employers and the police. Among the developed nations, the people of Canada spend more on life and disability insurance than almost

15 Ontario Ministry of Health, Some Principles of Individual Privacy and Data Dissemination (Toronto, July, 1979) 19. "In practice, the Ministry will produce on request of a subscriber, all records of payments made on his behalf during the preceding eight months."

any other nation. In so doing, they yield up substantial amounts of information about their health, habits and personal lives to non-medical personnel. Most insurance companies now require people seeking life insurance to sign a consent form which allows the company to check medical data with their physicians and to share this information with other insurance companies. The consent may also permit transfer of the information to a data bank operated by the Medical Information Bureau in the United States. Under The Insurance Act, an obligation is placed upon insurance applicants to disclose all material information concerning their health, but no obligation is placed upon the insurer to keep the information confidential.¹⁶

Employers often require prospective and current employees to disclose personal medical information. The Ontario government, for example, may require employees with high rates of absenteeism to submit to independent medical examinations. Those who refuse may face the prospect of suspension or dismissal.¹⁷

The police may also, on occasion, seek medical information in the course of criminal investigations or security checks. Usually, the results of these checks are unknown to record subjects. As the Ontario Medical Association stated in its brief to this Commission:

Information from personal medical histories has been used against people in employment, in public life and in business

16 The Insurance Act R.S.O. 1970, c. 224, ss. 122, 157, 257.

17 See Chapter X, "Government Personnel Records."

dealings. The potential for personal embarrassment, exploitation and suffering is so great that every effort must be made to ensure confidentiality of patient's medical records. 18

Recent revelations to the Krever Commission regarding unauthorized access to OHIP and hospital records by insurance companies and others have highlighted the need for stronger protections against non-medical use of health records.¹⁹ Clearer policies, controls on personnel with access to confidential records and increased physical security mechanisms might help prevent health record leakages to unauthorized non-medical users. The precise means of achieving this, together with a far greater elaboration of both the problem and the underlying principles, will be discussed by the Krever Commission in its report.

C. Legislation Affecting the Confidentiality of Medical Records²⁰

As we have mentioned, the traditional ethic governing the confidentiality of medical information known to a physician has been eroded by

18 Ontario Medical Association, op.cit., "Supplementary Comment to the Commission on Freedom of Information and Individual Privacy" (Toronto, October 24, 1977).

19 See, for example, Claridge, Thomas, "Insurance firms, 29 lawyers admit getting unauthorized medical data," Globe and Mail, October 13, 1978, 5.

20 The legislative interpretations of this section are based primarily on the County of York Law Association Brief to the Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario. We thank the Association for its work in preparing the brief and the Krever Commission for permission to use this material.

requirements in law that such information in certain circumstances be revealed to third parties. Such legislated "invasions" of the implicit confidentiality of medical information in the primary health care area fall into three categories; mandatory, investigatory and permissive reporting statutes. These legal erosions of privacy require closer examination to indicate the extent to which medical data is shared beyond the medical community, and within this study's terms of reference, to illustrate how Ontario government agencies receive authorized access to such data.

1. Mandatory Reporting Statutes

Mandatory reporting responsibilities appear to be well-known in the medical profession. In a survey conducted by the Osgoode Hall Law School,²¹ 90% of physicians questioned were found to be familiar with their statutory duty to report. The provisions of some of the better known mandatory reporting statutes²² are described in the following paragraphs.

The Highway Traffic Act:²³ Optometrists and all legally qualified medical practitioners are required to report all patients aged 16 and

21 The survey is reported in J.R. Carlisle and R.J. Gray, Medicine at Law (1978), H-53.

22 Although mandatory reporting primarily concerns medical personnel in the fulfillment of their medical duties, in some cases the reporting requirement is extended to members of the general public, who must report certain medical situations which come to their attention.

23 R.S.O. 1970, c. 202, as amended.

over having a condition that (in the opinion of the medical service provider) may make it dangerous for the person to drive. The Act specifies that doing so provides no action for breach of confidence and that the report is the privileged information of the Registrar.²⁴ Contravention of these provisions may be penalized by a fine of between \$20 and \$100.

The Venereal Diseases Prevention Act:²⁵ Physicians, persons in charge of the medical branches of various institutions (correctional, penal, educational, etc.) and superintendents/heads of hospitals or hospital sanatoriums are required to report the original diagnosis, treatment or care of venereal disease. Provision is made for the use of case numbers for identifiers (rather than a person's name) so that secrecy may be preserved. Contravention of secrecy may be enforced by a fine of \$200 (as well as any other action taken) and in the case of those employed in administering the Act, those revealing confidential information may be dismissed. The disclosure of information is permitted only to members of the family or in any judicial proceedings. Additionally, upon written request from the Director of the Division of VD Control, a physician is required to furnish any information in his/her possession with respect to the condition and treatment of a

24 In those cases where the licence is suspended due to the medical condition, the presence of the report and an indication of its severity is made "public" knowledge through the computerized driver record.

25 R.S.O. 1970, c. 479, as amended.

case of VD.²⁶ Administrators of VD clinics must permit the Director of the Division of VD Control to inspect clinic records in order to receive provincial grants.²⁷

The Public Health Act:²⁸ Any legally qualified medical practitioner (and those registered and practising under The Drugless Practitioners Act) shall notify the Medical Officer of Health of cases of specified communicable diseases.

The Vital Statistics Act:²⁹ All legally qualified medical practitioners (or the attending nurse, if there is no attending doctor) are required to report births, still births and deaths. Several classes of people are permitted access to the records, including authorized representatives of the government of Canada, its provinces, or those of another state or country.³⁰ While an oath of secrecy must be taken, there are no penalties for violation of the oath.

The Child Welfare Act:³¹ Every person having information about a child's abandonment, desertion, physical ill-treatment or need for

26 R.R.O. 1970, Reg. 819, s. 4.

27 Ibid., s. 8(a).

28 R.S.O. 1970, c. 377, as amended, s. 64.

29 R.S.O. 1970, c. 483, as amended, ss. 5, 14, 17(3).

30 R.R.O. 1970, Reg. 820, s. 66.

31 R.S.O. 1970, c. 64, as amended, ss. 45, 46.

protection shall report that information, notwithstanding its confidential or privileged nature. No action may be brought against the informant unless the information is given maliciously or without reasonable and probable cause.

The Coroners Act:³² Every person having reason to believe that a deceased person died under circumstances requiring investigation is to immediately notify the coroner of the facts and circumstances relating to the death. In addition, persons in charge of medical institutions are to notify the coroner of the death of any in-patients.

The Insurance Act:³³ An obligation is placed on all persons applying for insurance (life, accident and sickness) to disclose all material information concerning their health. There is no obligation placed on the insurer to keep this information confidential.

It may be further noted that regulations promulgated in most cases by the Minister of Health under The Ministry of Health Act,³⁴ may also

32 S.O. 1972, c. 98, as amended, s. 7.

33 R.S.O. 1970, c. 224, as amended, ss. 122, 157, 257.

34 S.O. 1972, c. 92, s. 6:

(2) The Minister in exercising his powers and carrying out his duties and functions under this Act,

(d) may collect such information and statistics respecting the state of health of members of the public, health resources, facilities and services and any other matters relating to the health needs or conditions affecting the public as are considered necessary or advisable, and publish any information so collected.

affect the confidentiality of medical records.

a) Problems with the Reporting Statutes

These reporting statutes contain clearly defined legal requirements. Three statutes state that the fulfillment of the reporting requirement cannot be considered a breach of confidentiality and cannot be grounds for legal action. However, the medical profession's uneasiness with this "role of informer" is evidenced by the low physician reporting rate of patients with medical conditions affecting driving ability (required under The Highway Traffic Act).

The assurance of confidentiality and the provision of penalties for unauthorized disclosure of medical information required under the statutes are in most cases either non-existent or of dubious value as a deterrent. The Vital Statistics Act, for example, is vague about the penalty (if any) for violation of the oath of secrecy. The Public Health Act does not preserve a limited confidentiality of reported communicable diseases. Considering the sensitivity of information about venereal disease, a \$200 fine for unauthorized disclosure of data collected under The Venereal Diseases Act may not be a sufficient deterrent (although there is provision that if the "informant" is employed in administering the program, s/he forfeits the job). The Highway Traffic Act provides for a fine of only \$20 to \$100 for unauthorized dissemination of reported information.

It is interesting to note that the majority of the reporting statutes impose greater penalties for the non-disclosure of required medical information to the authorized third party recipient (particularly the government) than for the unauthorized disclosure of such information when prohibited.

2. Investigatory Statutes

Investigatory statutes give specified agents, boards or review boards the power to have access to medical records and in some cases to compel medical personnel to provide verbal or written evidence of the related facts. Examples of such statutes relating to investigation and review of health care facilities and services include:

- . The Private Sanatoria Act
- . The Coroners Act
- . The Health Disciplines Act
- . The Workmen's Compensation Act
- . The Nursing Homes Act
- . The Homes for the Aged and Rest Home Act

Reviews of the quality of medical care may necessitate the examination of specific cases. In some instances, in order to check medical histories and results of care provided, records used must be identifiable.

The confidentiality of the medical information required to enforce the provisions of these statutes is not always assured. The Private Sanatoria Act, The Nursing Homes Act and The Homes for the Aged and Rest Homes Act contain no provisions governing confidentiality, thus leaving the common law (and the disciplinary provisions of The Health Disciplines Act) as the only recourse for abuse of confidentiality. Other statutes which do not have confidentiality provisions are The Mental Health Act, The Mental Hospitals Act, The Childrens Mental Hospitals Act, The Homes for Retarded Persons Act, The Homes for Special Care Act and The Community Psychiatric Hospitals Act. As well, The Workman's Compensation Act makes no provision restricting the use of medical information supplied by the employer.

It should be noted however, that some of the above-mentioned Acts do contain provisions penalizing failure to report or failure to provide the government access to information as required.

In addition to statutes governing the investigation and review of health care facilities and services, another class of statute allows courts and tribunals to compel disclosure of medical records and to order medical professionals and others to give testimony and produce evidence about health records. These statutes include:

- a) The Statutory Powers Procedure Act (S.O. 1971, s. 12)
 - (1) A tribunal may require any person, including a party, by summons,

- (a) to give evidence on oath or affirmation at a hearing;
- (b) to produce in evidence at a hearing documents and things specified by the tribunal, relevant to the subject matter of the proceedings and admissible at a hearing.

b) The Supreme Court of Ontario Rules of Practice (Rule 349)

Where a document is in the possession of a person not a party to the action and the production of such document at a trial might be compelled, the court may at the insistence of any party, on notice to such person and to the opposite party, direct the production and inspection thereof, and may give directions respecting the preparation of a certified copy that may be used for all purposes in lieu of the original.

c) The Evidence Act (R.S.O. 1970, c. 151, as amended)

52. (1) Any medical report obtained by or prepared for a party to an action and signed by a legally qualified medical practitioner licensed to practise in any part of Canada is, with the leave of the court and after at least seven days' notice, has been given to all other parties, admissible in evidence in the action.

52. (3) Except by leave of the judge presiding at the trial, a legally qualified medical practitioner who has medically examined any party to the action shall not give evidence at the trial touching upon such examination unless a report thereof has been given to all other parties in accordance with subsection 1.

The use of these statutes for breaching the confidentiality of medical information is not absolute. The major exception to the compelling of information would appear to be the doctrine of "work done in contemplation of litigation." In all three statutes there are provisions for the discretion of the court, and in the case of The Statutory Powers Procedures Act and the Rules of Practice there are the requirements that the document (or evidence) be admissible at a hearing or trial.

In the case of medical records, the judge's discretion may be used to deny admission of medical evidence on the grounds of medical confidentiality. In an Ontario Court of Appeal decision it was ruled that for The Evidence Act

The trial judge's discretion to admit a medical report must be exercised judicially. 35

On at least one occasion, a judge has used this discretion to disallow a breach of confidentiality of the psychiatrist-patient relationship

... based in part on the necessity that it would be a breach of the doctor's Hippocratic Oath, and in part on the necessity that a patient during a psychiatric examination must make full disclosure to the physician. 36

These factors could be readily extended to protect the confidentiality of the health care practitioner-patient relationship as a more general case. However, such recognition of confidentiality at the discretion of the judge must be used carefully. As the McRuer Civil Rights Commission concluded:

... the law cannot recognize any power in professional bodies to impose on their members declarations of secrecy (if they do) which would override the right of the individual to a disclosure of the truth before a court of justice. This would be an invasion of civil rights which ought not to be tolerated. 37

35 Kapulica v. Dumancic, [1968] 2 O.R. 438.

36 McRuer, J.C., Report of the Royal Commission of Inquiry into Civil Rights, Vol. 2 (Ottawa: Queen's Printer, 1968) 823.

37 Ibid., 823 (as cited in the County of York Law Association Brief to the Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario, op.cit., 31).

The basis for this conclusion is the belief that

The injury to justice by the repression of facts of corporal injury and disease is much greater than any injury which might be done by disclosure.

38

The belief that the pursuit of justice overrules privacy interests is not universally accepted. The injury done by disclosure includes not only the negative effects to the individual if non-relevant or inaccurate medical information is misused or misinterpreted, but also the injury to the public of possibly reduced quality of health care if the medical profession changes its record-keeping practices to guard against the disclosure of confidential information in court. It may be noted that one province, Quebec, and a number of American states have extended the doctrine of privilege to the physician-patient relationship.

3. Permissive Reporting Statutes

A number of statutes give health care practitioners the discretion to release information. One example is The Cancer Act, which permits the health care provider to report cancer cases to the Cancer Foundation and frees the provider from liability. (Note that while reporting cases to the Cancer Foundation is optional under The Cancer Act, it is mandatory under The Public Health Act.)

The major statute governing the optional release of information is The Public Hospitals Act,³⁹ which, together with Regulation 729⁴⁰ promulgated under the Act, governs access to hospital records. Similar legislation deals with other institutions, such as The Nursing Homes Act. The Public Hospitals Act⁴¹ stipulates that medical records are the property of the hospital and that hospital administrators are the custodians of the records. With respect to record access, the hospital board is forbidden, subject to certain exemptions, to permit any person to "remove, inspect or receive" information contained in any patient's record.⁴² Access must be granted, however, in response to a judicial order to an inspector engaged in an inspection under the provisions of the Act, to a coroner and his/her agents for the purpose of their investigations, and to an inspector from the College of Physicians and Surgeons of Ontario.

An authority to grant access on a discretionary basis is conferred in the following terms:⁴³

A board may permit,

- (a) the attending physician;
- (b) the administrator of another hospital who makes a written request to the administrator;

39 R.S.O. 1970, c. 378, as amended.

40 R.R.O. 1970, Reg. 729, as revised by O.Reg. 193/1972.

41 R.S.O. 1970, c. 378, s. 11.

42 Reg. 729, s. 48.

43 Ibid., s. 48(5).

- (c) a person who presents a written request signed by,
 - (i) the patient,
 - (ii) where the record is of a former patient, deceased, his personal representative; or
 - (iii) the parent or guardian of an unmarried patient under eighteen years of age;
 - (d) a member of the medical staff but only for,
 - (i) teaching purposes, or
 - (ii) scientific research that has been approved by the medical-staff advisory committee;
 - (e) a person with a written direction from the Deputy Minister of Veterans Affairs (Canada) or some person designated by him, where the patient is a member or ex-member of Her Majesty's military, naval or air force of Canada; or
 - (f) the Director of the Research and Planning Branch of the Department or his authorized representative approved by the Commission or an officer or employee of the Commission who is designated by the Chairman,
- to inspect and receive information from a medical record and to be given copies therefrom.

Failure to abide by these restrictions on access constitutes an offence under the regulations, which may result in a fine of between \$25 and \$100.

Under the legislation as presently interpreted, the use of consent forms signed by the individual for access to medical records is at the discretion of the board. This is of particular concern due to the widespread practice of, and in some cases legislated requirements for, the provision of medical information from hospital records to third parties. As stated earlier, informed consent is hardly possible in the absence of a right of patient access or right of patient control over further dissemination of information.

D. Conclusions

Two major issues arise from the foregoing discussion: control over transfer and dissemination of personally identifiable medical information, and patient access to records. However, these are not separate and discrete issues because the need for patient access arises from a fear that confidentiality of medical records cannot be absolutely guaranteed. Patients therefore need a means of ensuring that information about them is accurate and a means of finding out precisely what and with whom information is shared.

1. Information Transfer and Dissemination

1) Codes of information practices for medical records have been proposed by various bodies to better assure confidentiality of records. One such code, suggested by the Canadian Health Records Association, is shown in Table 2. Adoption of the CHRA code by "all agencies, organizations and persons involved in health data handling" has been encouraged by the Ontario Health Record Association.⁴⁴ Strict adherence to such a code would greatly minimize the risk of unauthorized or accidental disclosure of personal medical records. Implementation

44 Ontario Health Record Association, Brief to the Commission on Freedom of Information and Individual Privacy (Toronto, September, 1978) 4-7.

TABLE XI.2

CANADIAN HEALTH RECORD ASSOCIATION
CODE OF PRACTICE FOR SAFEGUARDING HEALTH INFORMATION

1. All individuals, institutions and organizations maintaining, handling or processing health information shall:
 - a) have written policies regulating access to, release of, transmittal and destruction of health information;
 - b) educate all their employees with regard to maintaining confidentiality of information, and have them sign a PLEDGE OF CONFIDENTIALITY. This procedure shall apply also to researchers, volunteers, contracted individuals and employees of firms and corporations performing contractwork.
2. Health information shall be accessed or released only for:
 - a) direct care use -- when requested by a physician or health care facility responsible for the direct care of the individual;
 - b) individual use -- when authorized by the individual or his legally authorized representative;
 - c) secondary use -- when requested by properly authorized persons or agencies;
 - d) legal use -- when required by law.
3. Requests for confidential information should be in writing; however, policies governing verbal requests shall be as outlined by the individual institution.
4. Any authorization for release of information shall be an original and specific as to source, content, recipient, purpose and time limitations. Reproductions of original signatures shall not be accepted.
5. Information released to authorized persons shall not be made available to any other party without further authorization.
6. Health information and records shall be kept in a secured area and not left unattended in areas accessible to unauthorized individuals.
7. In research, individual confidentiality shall be maintained in the handling of information and any reporting or publication of findings.
8. When health information is sent to any service organization for processing, the contract shall include an undertaking by the recipient that confidentiality will be maintained.
9. The authorized destruction of health information shall be by effective shredding, burning or erasure.
10. Any misuse of health information shall be reported to the responsible authority.

of such a code would necessarily involve clarifying the nature of authorized users and the circumstances of third party use. Current confusion over access to health records by the police (even when the purpose is to investigate fraud against the health plan or to notify law enforcement officials of gunshot wounds) clearly demonstrates the need to define precisely what is meant by authorized use. We anticipate that this topic will be examined at length by Mr. Justice Krever's report.

2) To further increase patient control over personal health record transfers, we propose basic changes in the consent process. Widely used blanket (all-encompassing) consents should be replaced by specific ones naming each potential recipient of personal medical information. Before asking someone to sign a consent for transfer, it should be common practice for the requestor to explain fully the purpose and extent of the transfer.⁴⁵

3) Confidentiality provisions of reporting statutes also require attention. While such provisions exist in most reporting statutes, the penalties for information abuse or further dissemination are in

45 This approach has been endorsed by the Ontario Health Record Association, op.cit., 5, "... we believe that members of the public should be aware that they have the right to limit authorizations by time and/or be content before signing the consent form, and further, they should understand what the ramifications of not doing so could be in terms of much more information being available to the requesting source than the patient may realize at the time."

most cases quite mild and are out of balance with penalties for non-reporting.

4) Security for medical records should be improved. Better technical safeguards protecting data as well as stronger controls on personnel with access to confidential records could prevent incidents of unauthorized access to medical information similar to those reported to the Krever Commission.

2. Subject Access

5) The health privacy issue most in need of attention in this province is subject access to medical information. A clear case for granting subject rights to medical information can be made. A number of experts in the health care field concur with our conclusion that greater knowledge of medical information leads to greater understanding, improves the health care provider-patient relationship, promotes physician accountability, and increases patient control over transfer and dissemination of confidential records.⁴⁶ As the American Medical Record Association has pointed out:

46 See, for example, Shenkin, Budd, M.D. and David C. Warner, Ph.D., "Open Information and Medical Care: A Proposal for Reform," (1975) 39 Connecticut Medicine 33-34; American Medical Record Association, Confidentiality of Patient Health Information: A Position Statement of the American Medical Record Association (adopted December, 1977); and Ontario Health Record Association, op.cit.

Many of the questions of confidentiality become moot if the patient is fully informed about the existence of information about his or her health care, has access to it and can exercise control over its dissemination.

47

The benefits of patient access to even the most sensitive medical records have been confirmed by the positive experiences of other jurisdictions. Included in this recommendation for broad subject access rights is the expectation that physicians and medical personnel will make every effort to explain the meaning of terms used in the record, to provide the patient with what the Ontario Medical and Hospital Associations have called a "fair interpretation" of medical information.⁴⁸

6) According to some, part of the difficulty in granting subject access is the unclear status of ownership of records. The Public Hospitals Act, for example, states that the record is owned by the hospital board, and the Ontario Medical and Hospital Associations have stated that "physicians own the records kept in their private offices respecting their patients."⁴⁹ However, the patient concerned surely has significant rights regarding the content of the record and its users. In our opinion, ownership is not a valid barrier to subject access.

7) In most cases, full access to medical records should present no

47 American Medical Record Association, Confidentiality of Patient Health Information: A Position Statement of the American Medical Record Association (adopted December, 1977) 10.

48 Ontario Hospital Association and Ontario Medical Association, op.cit., 2.

49 Ibid., 1.

problems. However, some medical professionals are concerned that unlimited and uninformed rights of access may prove harmful to patients psychologically and emotionally. To prevent such harmful effects, it has been proposed that in questionable cases, access be provided only through the patient's physician, who may exercise discretion as to the extent of disclosure.⁵⁰

Many experts have raised objections to such a proposition. Professor T. Ison, in a research paper prepared for this Commission, noted the risks of leaving the power of discretion to another physician:

... that the exercise of the discretion would depend less upon the judgment of the doctor about the characteristics of the particular patient than upon the opinion of the doctor about what the general disclosure rules should be ...

... that such a discretionary power would substitute the value judgments of the doctor for the value judgments of the patient about what the patient's best interests are. 51

In view of these risks and the positive experiences with direct patient access reported by St. Elizabeth's Hospital and other institutions, we recommend that in cases where access is deemed particularly harmful to the patient, that access be provided through the medium of a third

50 The arguments for subject access limited by an intervening physician chosen by the patient are summarized in Westin, op.cit., supra note 4, 289-293. Westin concludes that if the patient is not persuaded by a health professional, that another physician should determine the extent of access, the patient should have the right to see the record, "on the theory that there has already been a collapse of trust in the doctor-patient relationship and it would not be good medicine or in the patient's best interest to continue to refuse access at that point."

51 Ison, Terence G., op.cit., 102.

party, such as a legal representative, designated by the patient. We fail to see any situation in which access should be flatly denied.

E. The Health Care Number

The Ministry of Health is currently considering the introduction of a unique personal identifier in Ontario which would be known as the "health care number" and which would replace the OHIP number. The contentious factor in this proposal is the possible use of an existing and widespread identifier -- the Social Insurance Number (SIN) -- as the health care number, on the grounds of efficiency, minimization of cost, and interaction with other personal record systems which also use SIN.

As currently envisioned, the health care number (HCN) would be implemented in the following way. Initially, the HCN would simply replace the OHIP number in the OHIP system. It would then be extended to permit the integration of some existing file systems with the OHIP system into a central registry. Some existing systems suggested for integration are those concerned with Drug Benefits, Nursing Homes, Home Care, and Health Centres. In the future, the central registry could be extended to collect medical information not being collected at present and to provide a method for rapidly supplying condensed medical descriptions of patients to medical practitioners or treatment facilities.

1. The History of the Health Care Number

The idea of an individually identifiable number, specifically the SIN, for people using health services has relatively deep historical roots which are worthy of examination as a case study in the development of identification numbers.

In 1968, the Study on Numbering Systems for Person Identification in the Ontario Government⁵² recommended that the Social Insurance Number be adopted as the standard personal identifier in the Ontario government for the purposes of a central statistical data system. In the same year, the report, Health Research Uses of Record Linkage in Canada⁵³ recommended the adoption of a universal system using personal identifying numbers (such as SIN or birth number). In 1969, a report by the Ontario Council of Health on "Health Statistics" recommended that individuals in the Ontario Medical Services Insurance Plan (OHSIP) and the Ontario Hospital Services Commission (OHSC) be identified by a number common to all systems, and that SIN be used to identify individuals in addition to standard identifiers used at that time for administrative purposes. However, when OHSIP and OHSC were merged to form OHIP, the 8-digit contract holder identifier of OHSC was used for

52 Ontario Statistical Centre, Study on Numbering Systems for Person Identification in the Ontario Government (Toronto, 1968).

53 Medical Research Council of Canada, Health Research Uses of Record Linkage in Canada: A Report to the Medical Research Council of Canada (Ottawa, 1968).

the OHIP number rather than the SIN number of the contract holder.

In 1970, the report of the Ontario Council of Health on "Health Statistics"⁵⁴ recommended that for the purpose of health statistics, a central statistical agency -- the "Health Statistics Agency" -- be formed to plan, coordinate and direct the collection of data for the health statistics system and to serve as a central access point for the decentralized health statistics system.

A further report by the Ontario Council of Health, on the Role of Computers in the Health Field, recommended that a universal unique code be provided to residents to facilitate efficient data linkage.⁵⁵ The report stated that "The SIN is becoming the most commonly accepted procedure for this purpose." It also dealt extensively with the ramifications of linked health records in terms of the measures necessary to protect the privacy and confidentiality of medical records in a linked system. Two years later, the Task Force on Privacy and Computers examined the general question of personal identifiers in Canada and acknowledged that the seriousness of the issue warranted further public discussion before a universal unique personal identifier could be seriously considered. It also warned of the trend towards the use of

54 Ontario Council of Health, Health Statistics, Report Part II: Implementation of a Health Statistics System (Toronto, 1970).

55 Ontario Council of Health, Health Care Delivery Systems, Supplement Number 9: Role of Computers in the Health Field (Toronto, 1970).

the SIN as a "de facto" universal unique personal identifier.⁵⁶

Two further studies on the issue of identifiers in the health field were undertaken in 1974. The first explored the implications of using a plastic identity card for OHIP.⁵⁷ While it concluded that an embossed plastic card should be used for individual identification for OHIP purposes, it recommended that use of such a card be delayed until the issue of a unique personal identifier was resolved. A concurrent study, The Implications of Using a Personal Identifier in the Ministry of Health,⁵⁸ recommended that the Ministry adopt and standardize the use of the SIN for all its people-oriented programs and that the possession of a SIN become mandatory for all provincial residents.

Subsequently, in March 1975, the Ministry of Health recommended to the Cabinet Committee on Social Development that the Social Insurance Number be adopted as the unique personal identifier for ministries in the social policy field. The Committee decided, however, that this proposal should not go forward. In early 1977, Cabinet authorized the

- 56 Canada, Departments of Communications and Justice, Task Force on Privacy and Computers, Computers and Privacy (Ottawa, Queen's Printer, 1972).
- 57 Ontario Ministry of Government Services, Management Consulting Services, A Study of the Implications of Using a Plastic Identifying Card for the Health Insurance Plan (Toronto, 1974).
- 58 Ontario Ministry of Government Services, Management Consulting Services, A Study of the Implications of Using a Personal Identifier in the Ministry of Health (Toronto, 1974).

Ministry of Health to announce the proposal to use the Social Insurance Number in the Ministry of Health as a unique personal identifier.

An OHIP Task Force on the health care number later recommended that OHIP undertake the initial registration and that integration with other Ministry programs occur during the six months following the initial registration. The proposal for improved record linkage was supported by the Ontario Council of Health in its 1977 report, Health Research Priorities for Ontario,⁵⁹ in which it recommended that "a system of health-related record linkage in Ontario, compatible with systems in other provinces, be introduced as soon as technical and legal measures have been devised to preserve the privacy of individuals."

In September, 1977, the Ministry of Health's submission to this Commission indicated that public announcement of the health care number would follow shortly thereafter.⁶⁰ However, after consultation with this Commission, the Ministry decided to postpone institution of the health care number project. The stated reason for this postponement was the Ministry's desire to consider the findings of both this Commission and the Krever Commission in the HCN decision. However, public announcement of the proposal did occur. On May 6, 1978, the London Free Press reported the following:

59 Ontario Council of Health, Health Research Priorities for Ontario (Toronto, 1977) 3.

60 Ontario Ministry of Health, Submission to the Commission on Freedom of Information and Individual Privacy, September 7, 1977.

Pending the outcome of the Krever Commission and one on privacy and information ... Ontario may be embarking on a new patient identification system. Health Minister Dennis Timbrell said in London this week he has Cabinet support to go ahead with a unique form of plastic card that will contain social insurance numbers.

61

Further consideration by the Ministry of Health on the implementation of the health care number system apparently awaits the findings and conclusions not only of this Commission and the Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario, but also of the Standing Committee on Health Care Costs. The latter's report is expected to provide a more precise cost-benefit analysis of the health care number proposal, and to discuss the implications of the reports by the other two Commissions.

2. A Review of the Rationale for the Health Care Number

Two reasons are officially cited as the basis for implementing a health care number. It would enable the unique identification of individuals within existing programs (primarily OHIP), and it would aid data linkage between programs. These arguments are generally made to support the adoption of any unique personal identifier.

- 61 Insofar as it was not the Ministry's intention to make a public announcement at this time, it is surmised that this information came in a post-speech discussion period scheduled after Minister Timbrell's speech at the Spring General Meeting of the London and District Academy of Medicine.

The primary identification method, among others, used by the Ministry of Health is the OHIP number. However, as multiple listings increase and as new demands are placed on OHIP and other health systems, the OHIP number has become increasingly inadequate for the task. An individual may acquire more than one OHIP number throughout his/her lifespan, due to the natural change from a dependant to an independant adult status, and due to the Ministry's errors in issuing multiple OHIP numbers to the same individual. In addition, the OHIP number identifies "contracts," and thus may refer to one or more persons (i.e., the contract holder plus dependants). The problem has also been aggravated by the recent need to "recycle" OHIP numbers. To avoid false matching, OHIP numbers are now processed with auxiliary information, such as birthdate, name and sex. These supplementary identifiers have proven inadequate due to errors in transcription and to a common subscriber practice of using various name forms, such as Bill, Billy, Will or William.

The Ministry cites improved efficiency and accuracy as a major reason to implement a unique personal identification system, which would eliminate the need for extra cross-checking, storage and processing of multiple entries for the same individual. However, because no study or project has been undertaken to determine the specific level of accuracy obtainable with existing identifiers, it is difficult to compare such levels with any proposed health care number identification system, inasmuch as such a system would require exorbitant "quality controls"

to obtain total accuracy. To illustrate this potential problem, we note that the Social Insurance Number is still considered only 98% accurate even with the strictly tightened controls and checks implemented in 1974. Because the OHIP system has effectively met its requirements using the present identifiers, and because a unique personal identifier would only marginally increase system accuracy, OHIP management has stated that the few perceived benefits would not make the switchover cost-effective within the OHIP organization itself.

Despite the lack of empirical research and the doubts of OHIP management, the introduction of a unique personal identifier system has been deemed necessary to satisfy "overall Ministry considerations" and to pave the way for proposed changes to the OHIP system, for example, in the areas of itemized cost statements or collection methods. The proposed Individual Itemized Health Cost Statement Program⁶² would provide a complete and accurate health cost listing by benefits received (as billed to OHIP) to each individual subscriber. Such a system would obviously be facilitated by the introduction of health care numbers unique to each subscriber.

The second major justification given by Ministry officials for the health care number is the increased need to integrate and link systems

62 This is a universal system that would be fairly similar to the existing verification system in which contract holders (30,000 per month) receive a listing of services on their behalf billed to OHIP (Note that there are strict privacy safeguards built within this system).

utilizing the same identifier. This integration could enhance statistical use of existing data systems for both research purposes and policy decision-making. As well, much duplicated information gathering by the numerous separate Ministry programs could be eliminated. The linkage of Ministry-held data systems has and is being achieved using existing methods, but only on a one-shot project basis. A health care number could facilitate an automated program for linking file systems either on an ad hoc or long-term basis.

However, the proposed health care number would not solve many problems which now inhibit large-scale cross-linkage and integration of files. First, prior to any linkages, file systems would have to be "cleaned up" and duplicate entries eliminated. Second, the incompatibility of existing systems due to differing orientation, specification and structure (most systems were originally designed for operational, administrative or accounting purposes) would still exist and would render the integration of data from such differing contexts of dubious value or accuracy, particularly in a statistical context. In addition, individual programs have different levels of information "quality" and detail. For example, a number of different code classifications exist for some medical diagnoses, which would present major problems for the meaningful use of integrated systems. Because of these problems, a move toward system integration (utilizing a health care number or other mechanisms) would require massive restructuring, verification and conversion of the majority of data systems involved. Therefore, no

matter what the outcome of the health care number decision, the Ministry of Health can consider only a few fairly compatible computerized systems for immediate integration into a "Health Care Registry."

Several studies⁶³ have investigated or reviewed alternative unique personal identifiers for use as the health care number, ranging from existing numbers -- such as birth registration number, SIN and drivers licence number -- to new derived or assigned unique personal identifiers. These studies suggested that the favoured alternatives were either the SIN or a new assigned identifier. The latter's advantage is that it could be independently issued, verified and quality-controlled by the Ministry. In addition, a new identifier's uses could be more easily limited to those related to the health field.

On the other hand, the Social Insurance Number has the benefits of an established identifier, already obtained by 65% of Ontario residents and already subject to established issue and verification mechanisms through the federal Unemployment Insurance Commission. The SIN is perceived as desirable in part because of its wide usage in other government programs. For example, a health care number which is the same as the SIN would make a proposed pro-rated payroll billing system (to replace the current premium system) significantly more efficient

63 Primarily, the Ministry of Government Services Study of the Implications of Using a Personal Identifier in the Ministry of Health, op.cit., and Ministry of Government Services, Health Care Number/Unique Personal Identifier Project, PE44.

by permitting direct linkage with the federal tax file system, enabling more automatic and accurate assessments for billing purposes.⁶⁴

3. Privacy and the Use of the SIN in the Health System

A major effect of using an established UPI such as the SIN for the health care number is the increased ease of linkage or integration with existing or proposed systems already using it. The possibility of linkage with the health care systems of other provinces using the same identifier played a major role in Ontario's decision to use the SIN for the proposed health care number. However, despite encouragement by the federal government, other provinces considering the use of the SIN as the UPI in the health area appear to have resisted to date. Only the benefits of linkage with federal government information systems and other Ontario data systems remain.

Federally, the possible interactions for information linkage occur in the areas of financial information (for possible OHIP billing purposes) and medical information statistics (for Statistics Canada). Both of these linkages pose problems for patient control over transfer of personal medical information. At present, such proposals for linkage

64 It should be noted that the SIN is not the primary identifier used within the tax system.

do not consider the possibility that patients may wish the rights both to deny OHIP access to tax records, and to authorize the extent of information transfer to Statistics Canada.

Provincially, in addition to the integration and linkage leading towards the "Health Care Registry" in the Ministry of Health, an integrated Health Care Registry using the SIN as identifier would greatly enhance the ease with which medical record data could be linked with personal information held by other ministries. A significant amount of data sharing (for operational or research purposes) already occurs within the social policy field (the Ministries of Labour, Health, and Community and Social Services). As a reflection of further data sharing possibilities, it was originally suggested to the Cabinet Committee on Social Development that the SIN be used as the UPI in the entire social policy field. Such proposals for data linkage raise further concerns about the confidentiality of medical records. Considering the present situation in Ontario, in which the adequacy of current medical record confidentiality is being questioned and in which present information transfer arrangements are being reviewed, the privacy, confidentiality and security aspects of a move towards a more integrated "Health Care Registry," particularly one using the SIN, require careful consideration.

Given these concerns, we recommend that any proposed health care number in Ontario be specifically associated with medical uses, and not with the broader uses currently envisioned for the SIN. We therefore suggest

that the Ministry of Health initiate its own unique personal identifier in any proposed health care number system,⁶⁵ rather than a universal identifier such as the SIN. Efforts to control data dissemination would only be enhanced by the use of discrete identifiers for specific purposes. Furthermore, data linkage would still be possible (for essential functions such as epidemiological research) without changeover to a SIN-based system. The possible administrative costs and inconvenience resulting from the maintenance of a separate identification system for medical records is a small price to pay for public peace of mind about the potential misuse of such records.

65 This recommendation concurs with one of the Ontario Health Record Association, op.cit., "That a unique identifier be developed for health data alone and utilized among health organizations for the linkage of health information to the benefit of the patient; that this number be separate and distinct from either the OHIP number or the Social Insurance Number and never used in conjunction with them, and; that legislation ensure that this health data is maintained in an independent, ethically controlled, separate data bank to protect against its linkage with other social systems. The Ontario Medical Association, op.cit., has also commented, "That in the collection or transmission for statistical purposes of information from medical records, the name, address, Social Insurance Number, OHIP number and any other patient identifier be deleted."

CHAPTER XII

LAW ENFORCEMENT

A. Introduction

The gathering and handling of personal information by law enforcement agencies raises particularly difficult issues of privacy protection. In the first place, it is inherent in the nature of law enforcement activity that highly sensitive personal information will be gathered and deployed against the personal interests of the data subject. Data will be gathered without the knowledge or consent of the data subject by methods which would, under any reasonable standard of measure, be considered to be invasive of personal privacy. Public tolerance of these invasive practices is premised, of course, on the need for effective law enforcement as a means of preserving public order. On the other hand, it is widely accepted that there are limits to the extent to which the public interest in privacy protection should be sacrificed to the public interest in effective law enforcement.

A full account of the historical process by which these limits have been delineated would require a comprehensive survey of the evolution of the legal limitations imposed on the powers of investigation and surveillance of the police. The ability of law enforcement officials

to invade the privacy of individual citizens has been circumscribed to some extent in laws governing powers of arrest, search and seizure, and electronic surveillance¹ -- laws under which the courts are the ultimate arbiter of the balance to be achieved between privacy protection and effective law enforcement. More than this, however, there are widely shared, if differing, assumptions about the extent to which civil libertarian values should act as a restraint on the investigative and intelligence gathering activities of law enforcement agencies. An exploration of the appropriate reconciliation of these conflicting values would carry us into an examination of fundamental questions concerning the relationship between the citizen and the state and the proper role of law enforcement activity in a democratic society.

It was not our mandate to examine and pronounce upon these profound and deeply philosophical questions. We have not attempted to study, for example, the use by law enforcement authorities of illicit techniques for the gathering of personal information. A fruitful examination of the factual underpinning of such questions is beyond the reach of a study team such as ours and is, in any event, a matter which has been examined and is currently being examined by various Royal Commissions.² Nor have we addressed the vexing question of the

1 See generally, S. Cohen, Due Process of Law (Toronto: Carswell, 1977) 61-105.

2 Royal Commission into Metropolitan Toronto Police Practices (Morand Report) (Toronto: June 1976); Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Security and Information (Ottawa: Ministry of Supply and Services Canada, 1980); Quebec Commission of Inquiry into the RCMP (Keable Commission, 1978).

extent to which evidence gathered by law enforcement authorities by illicit means should be admissible in a court of law for the purpose of prosecuting accused persons.³

What we have attempted to do is to develop an understanding of the nature and structure of records which the police typically maintain about individuals and to highlight the privacy concerns surrounding their accuracy and use.⁴ In this respect, it is important to note that it is not only "criminals" who are the subjects of law enforcement information. The names of victims, suspects, arrested but unconvicted persons, and witnesses, for example, also appear in such files. Moreover, it is important to note that law enforcement files are used for purposes other than the prosecution of offences. Security checks, criminal record checks and other uses of such files are of interest to law abiding citizens and represent situations in which inaccurate data or misuse of files may unfairly harm an individual, whether or not s/he has ever engaged in criminal activity.

3 As a general rule, evidence garnered by unlawful means is admissible under Canadian law. See *R. v. Wray* (No. 1), [1971] S.C.R. 272. Wiretap evidence obtained without proper authorization is, however, specifically rendered inadmissible by the provisions of the Criminal Code. See Invasion of Privacy Act (Criminal Code Part IV.1) S.C. 1973-74, c. 50, as amended by S.C. 1976-77, c. 53.

4 For similar studies of police information systems in other jurisdictions, see Westin, A.F. Databanks in a Free Society (New York: Quadrangle, 1972) 47-65, 77-88; Rule, J., Private Lives and Public Surveillance (New York: Schocken Books, 1974) 44-96; O'Connor, K.P., Federal Police Records (Sydney, N.S.W., Australian Law Reform Commission, 1979); Report of the Committee on Data Protection (Lindop Committee) (Cmd. 7341, 1978) 79-88.

It seems evident that the fair information practice principles articulated elsewhere in this report are, for the reasons suggested above, applicable to law enforcement information systems and that some mechanism for implementing such principles in this context, without unduly impairing the effectiveness of our law enforcement agencies, is therefore necessary. After briefly describing the organization of policing activities within the province, we will turn to a description of the records of information systems of the Ontario policing authorities. We have not attempted to examine the information systems of federal policing authorities, nor have we been able to examine the extent to which law enforcement information is shared with foreign police forces or international organizations such as Interpol. Parenthetically, we should note that our account of existing information systems is based almost exclusively on interviews with law enforcement officials rather than first-hand observation of the systems themselves. In the last section of this chapter, we will offer an assessment of the possible means by which fair information practice principles might be applied to law enforcement files.

B. Organization of Policing in Ontario

Policing in the province of Ontario is carried out by three police forces:

- 1) The Ontario Provincial Police (OPP), who are the Crown force, responsible for policing of highways and rural areas and

also for lending specialized support to smaller municipal police forces. It consists of 180 detachments around the province, with headquarters in Toronto.

2) 128 municipal police forces, ranging in size from 5,300 uniformed officers in Metropolitan Toronto to a single officer in some small towns.

3) The Royal Canadian Mounted Police (RCMP), who are concerned with certain specialized aspects of law enforcement in the province in cooperation with other forces.

In the Ontario government, responsibility for law enforcement rests with the Solicitor General, who administers the Police Act.⁵ Through the Solicitor General, members of police governing authorities are appointed. The Ontario Police Commission monitors policing standards in the province and is responsible to the Solicitor General. The Commission also provides training to police forces at the Ontario Police College, and technical advice. It is not uncommon for investigations to be carried out through joint efforts of these police forces. We were unable to discern any fixed pattern in these efforts, however. It is fair to say that all three levels may retain overlapping or duplicate records on an individual or incident.

5 Police Act, R.S.O. 1970, c. 351, as amended by S.O. 1972, c. 1, s. 97.

C. The Sources of Law Enforcement Information

For purposes of discussion, it is useful to distinguish between two major types of law enforcement information gathering activity: the investigation of specific occurrences, and the gathering of "intelligence" information. Intelligence may in turn be considered in two aspects: criminal intelligence -- where ongoing efforts are devoted to bringing continuing criminal operations before the courts, as with prostitution or loan sharking -- and security operations, which are designed to identify and prevent the realization of threats to the government and the political stability of the province. This latter category is comprised of subversive activity and threats on the lives of important public officials. The distinction between occurrence investigation and intelligence gathering is that the former refers to a specific incident, and the latter is connected more to a pattern of occurrences, or to the prevention of occurrences.

In addition to personal information collected through occurrence or intelligence investigations, certain types of personal information are generated through the process of law enforcement. Police records, which include records of arrest, prosecution, disposition and sentence are the examples of primary concern. Documentation relating to search warrants and wiretap authorization, even where they are not granted, might also be considered personal records connected with law enforcement. Court transcripts of trials, appeals and related proceedings are records containing personal information generated by the law enforcement process.

The potential sources of investigation and intelligence information are virtually unlimited. Police use whatever sources they can to trace suspects and witnesses or to acquire evidence. The major sources of information, of course, are individuals voluntarily supplying information to the police, whether they be witnesses, victims, persons suspected of criminal activity or persons who for some other reason are in possession of useful information.

Where a source of information is unwilling to volunteer it, the only legal recourse (prior to the trial of an accused person, at which time witnesses may be compelled to give evidence by a subpoena) is to obtain a search warrant granting the police the right to enter a named building, receptacle or place. A justice of the peace issues the search warrant upon being satisfied that "there is reasonable ground to believe" that evidence bearing on the actual, suspected or intended commission of a crime⁶ would be found on the premises. A search warrant is not issued for what the courts have called a "fishing expedition."⁷ This means that there must be reasonable certainty of both the location and the object of the search. The mere suspicion or curiosity of a peace officer would not satisfy the justice of the peace that it would be proper to issue the warrant. The search warrant is only useful, however, to obtain physical evidence. The

6 Criminal Code, R.S.C. 1970, c. C-34, s. 443(1).

7 Re Purdy et al. and The Queen (1972), 8 C.C.C. (2d) 52.

police have no general power to compel individuals to respond to questions and inquiries.⁸

Should the police wish to obtain information by engaging in electronic surveillance of individuals, it may be necessary for them to obtain judicial authorization under the provisions of Part XIV.1 of the Criminal Code. These provisions were introduced by the Protection of Privacy Act in 1974,⁹ to regulate the collection of information from private communications via electronic means, i.e., wiretapping. As a general rule, judicial authorization for the use of this method (subject to certain exceptions) is required. Subsequent notice to the subject of the interception must be made in certain circumstances. The tape recording resulting from a wiretap may not be produced as evidence if it has been obtained without proper authorization. Further, the statutory provisions permit an award of damages against enforcement personnel engaging in unlawful surveillance.

According to one of our police interviewees, the main sources of personal information, apart from individuals, are public and private institutions such as government ministries and agencies, banks, hospitals, telephone and credit companies, and other law enforcement agencies, the latter term being broadly construed to include social

8 See generally, Cohen, op. cit., 71-80.

9 See generally, M. Manning, Protection of Privacy Act (Toronto: Butterworths, 1974); Wiretap Law in Canada (Toronto: Butterworths, 1978); D. Watt, Law of Electronic Surveillance in Canada (Toronto: Carswell, 1979).

service agencies such as the Children's Aid Societies and the John Howard Society. Without more elaborate inquiries than we have been able to undertake, it is not possible to assess the extent to which these institutional sources of information are utilized by the police. Illustrations of the use made by the police of information held by ministries of the government are indicated elsewhere in this report. Thus, Ontario police officials have direct access to the vehicle and driver licensing files maintained by the Ministry of Transportation and Communications.¹⁰ The particular case of the utilization of medical records maintained by both public and private institutions for law enforcement purposes is currently undergoing extensive study by the Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario. Further, it may be noted that the general subject of governmental access to personal information maintained by private institutions has been thoroughly examined by the U.S. Privacy Protection Study Commission.¹¹ In essence, that Commission recommended that such access be permitted only where legal process in the form of a warrant or subpoena has been followed.

An interesting illustration of the problematic aspects of police access to the documents of private institutions came to our attention in the course of our research. The Commission was informed by the Board of Trustees of one of Ontario's libraries that some libraries had received

10 See Chapter XV.

11 Privacy Protection Study Commission, Personal Privacy in an Information Society (Washington, D.C.: USGPO, 1977) 345-392.

requests from police for access to the circulation records of particular borrowers. While The Public Libraries Act¹² provides that any person may at any reasonable time inspect the libraries records, the Board in question expressed concerns that access of this kind constituted a threat to the privacy or intellectual liberty of the individual, and instructed the staff to refuse to make such materials available in the absence of a proper search warrant.

Apart from civil libertarian concerns of the kind raised by the above Board, however, this example does make the point that the police seek information from a perhaps surprisingly broad range of private institutions. With the exception of search warrants or situations in which authorizations for electronic surveillance are required, determination of when and how to use such methods and sources are within the sole discretion of the police.

D. Systems of Personal Information
Record-Keeping by the Police

1. Introduction

There are three major categories of records about individuals which are held by police agencies. They are:

12 The Public Libraries Act, R.S.O. 1970, c. 381, s. 26.

1) Occurrence and investigation reports, which contain notes and other documentation about specific cases or incidents investigated by the police. These may or may not result in criminal proceedings and include reports on traffic accidents, family disturbances and the rich variety of other complaints investigated by the police.

2) Criminal history and identification records, which contain identifying material -- such as a physical description, fingerprints, address, date of birth and photographs -- and historical material, such as notations of arrests, detentions, indictments, "informations" or other formal criminal charges, any disposition arising therefrom, and sentencing, correctional supervision, and release data.

3) Criminal intelligence reports, which contain identifying material, data concerning past criminal activity, arrests, convictions, sentences, parole, probation and other information about the associates, movements, business and personal activity of the data subject thought to be useful by the police. This information may be of a highly speculative nature. It may relate to individuals known to have been involved in criminal activity in the past, or to individuals suspected of being involved in, or for some reason suspected of being prone to, participation in criminal or subversive activity.

In Ontario, police record-keeping systems are both manual and automated; some are centralized, and others are decentralized with no effective coordination among them. Each of the 180 OPP detachments keeps its own

occurrence reports and criminal records; these are only partially indexed -- occurrence reports by the OPP, and criminal records by the RCMP. Much personal information is centralized through the national police computer -- CPIC (Canadian Police Information Centre). In Ontario, all police forces, the Ontario Police Commission, the Centre of Forensic Sciences, and the Coroner's Office have CPIC terminals. Another central computer-stored bank of personal information is the federally coordinated ACIS (Automated Criminal Intelligence Service). Intelligence information is stored on ACIS and used by the 28 Ontario police forces and 8 affiliated bureaus which are members of CISO (Criminal Intelligence Service of Ontario).

After considering in greater detail the major types of records maintained by police forces in Ontario, we will return to a more complete account of the two centralized and computerized law enforcement information systems.

2. Occurrence and Investigation Reports

In most cases, an occurrence or investigation report is initiated upon the complaint of a private citizen, or the observation of a police officer. At OPP detachments, this is initially entered in the "occurrence book," in which is noted the time, the nature of the occurrence, the officer assigned to the investigation and the disposition made of the matter. An occurrence report is prepared for each occurrence referred to the detachment.

These reports are then filed in an "open occurrence" file and a name index card is prepared by which the occurrence report may be accessed. The name on the name index card could be the name of the victim or the name of the suspect. Occurrence reports themselves are filed by number and are not therefore easily retrieved. The cards are cross-indexed to link the names of different persons involved in the same occurrence and the cards may be used to trace individuals in the course of subsequent investigations. Once the occurrence has been investigated and satisfactorily dealt with, it is filed in the "closed occurrence" file and all occurrence reports pertaining to a single investigation are brought together in a single file.

Much of the same information is contained in the notes of the police officer. While these notes may be considered personal preliminary observations collected to assist the officer's memory, they may be required to be produced in court proceedings as evidence; as part of the information which an accused person is entitled to know, they may be subpoenaed for production in court. Police notes are kept as long as the officer remains on the force. After the officer leaves the force, notes are retained in the Quartermaster's Stores, in case they are needed for the continuation of a particular investigation.

A report location index card is prepared on the basis of occurrence reports for central storage and use at the OPP headquarters in Toronto. These are made available to other police forces and in appropriate cases to insurance companies engaged in the investigation and

settlement of claims.

Reports of 12 categories of "major occurrence" are distributed to headquarters in Toronto, in addition to two reports of occurrence which may be relayed at the discretion of the detachment commander. The 12 occurrence categories are: abduction, armed robbery, arson or suspected arson, break and enter relating to property worth over \$5,000, extortion, gambling, possession of criminally-obtained property worth over \$5,000, rape, sudden death or homicide other than in motor vehicles, theft over \$5,000, suspected fraud, and attempts to commit any of these crimes.

The two discretionary reports relate to drug offences, and any unusual occurrence such as a demonstration. Even when a drug occurrence is not deemed "major," reports of it are sent to the federal Department of Health and Welfare. When a report concerns a death from other than natural causes, a copy is distributed to the Chief Coroner's Office. In the case of a hunting accident, a report is sent to the regional office of the Ministry of Natural Resources. In the case of a forest fire, one is sent to the regional office of the Fire Control Branch of that Ministry. Where arson, suspected arson, or a fire fatality is involved, a copy of the report is forwarded to the Fire Marshall's Office in Toronto.

An examination of occurrence reporting in a major metropolitan centre indicates a similar pattern for the initial reporting stages. Among

the police divisions within that force, there would appear to be a greater coordination and centralization of record-keeping than exists among OPP detachments. As a result, the indexes to the reports allow greater use to be made of decentralized reports by the investigating officer assigned to each case. A central computerized index allows access to all occurrence reports by crime category, the names of victims and complainants, the person charged, and the location, date and time of the incident. A card index is related to this computerized index and contains descriptions of property involved in crimes.

3. Identification Files

Identification files are typically maintained by an identification unit within a police force whose function is to assist police investigators to assemble and identify physical exhibits and to identify suspects. Files of an identification unit would therefore typically contain fingerprints, physical descriptions and photographs of convicted criminals and suspects who have been previously charged. Under the Identification of Criminals Act,¹³ any person who has been charged with or is under conviction for an indictable offence may be subject to identification procedures, which normally include fingerprinting and photographing. These records may be published for the information of others engaged in the administration of the law. The police also

13 R.S.C. 1970, c. I-1.

fingerprint other persons (with their permission) who have been in the vicinity of a crime, where they wish to eliminate the prints of these persons from those taken at the scene. Such prints are called "elimination prints," and it is our understanding that they may occasionally be kept on file to avoid the necessity of taking fresh prints should there be a recurrence of the crime. An identification unit also maintains files on specific investigations in which it has been involved which may include criminal occurrences or serious traffic accidents. With respect to elimination prints, we believe that there should be a firm policy that such prints be returned to the individuals within a specified period after the completion of the investigation.

Identification information is shared, to some extent, with the RCMP and finds its way into the CPIC system. For indictable offences, identifying data such as photographs, physical descriptions and fingerprints are sent to the RCMP in Ottawa. Fingerprints are used thereafter for identification purposes when a person asks to examine his/her record. This is not the case, of course, for summary conviction offences for which all identifying material is kept locally in hard copy. Although fingerprints may be included in these files, they do not form the basis for assuring identification should a person wish access to his/her own file.

Some identifying material collected in occurrence reports and through the investigation also finds its way onto CPIC. The CPIC system permits the entry of information which assists in the identification of persons, vehicles and property.

A CPIC entry about a person indicates that the individual is wanted pursuant to a warrant for arrest or other reason, or that the person has been reported missing. Identification information of some kind normally accompanies such entries. A typical CPIC entry concerning vehicles and property describes the item in question and indicates the reason why police have been alerted. In the case of vehicles, a car may have been abandoned or stolen, or used in connection with a crime, or simply be a vehicle "for observation." It is only in this latter category that personally identifiable information may be relayed -- an entry is available for remarks, and a typical remark might name the vehicle's owner. The only personal information which may appear in a "property" report names the owner of missing securities.

4. Intelligence Files

Perhaps the most sensitive information maintained by police forces is that collected during intelligence work. Intelligence information, broadly defined, is simply information which is not related to the investigation of a specific occurrence. The information normally relates to patterns of conduct of identifiable individuals or groups and is often produced by direct surveillance of them by the police. Beyond this, however, it is difficult to satisfactorily define the term or to reach agreement as to the proper scope of intelligence gathering activity.

Some intelligence gathering has as its objective the maintenance of information which might ultimately be useful in investigating specific offences. Thus, information relating to the activities of habitual and dangerous criminals may be maintained in the expectation that it may subsequently prove pertinent in investigating offences perpetrated by such individuals. In some cases, such information may be useful to the police in an attempt to prevent the occurrence of a crime.

Intelligence gathering also occurs for "security" purposes, i.e., in an attempt to prevent the occurrence of politically motivated violence and other types of subversive activity, and to ensure the safety and security of government institutions and personnel.

In broad general terms, then, it may be said that there are two categories of intelligence information gathered by the police in Ontario -- criminal intelligence and political or "security" intelligence. We will briefly describe the information systems relating to each of these types in turn.

a) Criminal Intelligence

Criminal intelligence is gathered by police officers at all levels. There is a criminal intelligence network in Canada -- the Criminal Intelligence Service Canada (CISC) -- with nine affiliate bureaus in

the provinces. The Criminal Intelligence Service for Ontario (CISO), staffed by police officers, acts as a repository of information gathered by CISO members, all of which are law enforcement agencies active in Ontario. CISO accounts for approximately 50% of the data in the CISC network. The member bureaus, as well as each police organization constituting the membership of a bureau, subscribe to a strict constitution dictating the circumstances in which intelligence information is to be shared.

The membership of CISO consists of police forces and individual officers from those forces who are engaged in intelligence work. The criterion for membership of police forces in CISO is that full-time criminal intelligence files are kept by the force. All member bureaus must agree to the membership of new applicants. While the 28 "full member" bureaus are police organizations (including the OPP and the RCMP), and all new members probably will be, eight other organizations were granted affiliate status at CISO's inception:

- . Canada Employment and Immigration Commission
- . Insurance Crime Prevention Bureaus
- . Ontario Fire Marshall's Office
- . Ontario Securities Commission
- . Ontario Superintendent of Insurance
- . Toronto Port Police Force
- . Canada Customs Intelligence
- . Ministry of Consumer and Commercial Relations.

The affiliate status of these groups means that they are not granted full privileges in the organization. Thus, affiliate members may be excluded from CISO meetings. Of more interest here is the fact that access to CISO information which has been requested by an affiliate is

made available only with the contributor's agreement. Information not solicited by an affiliate may be passed on at the initiative of CISO personnel, but only with the agreement of both the head of CISO and the contributor.

As mentioned earlier in this chapter, the definitional distinction between intelligence and regular investigative work turns on some measure of specificity. Information gathered in the course of investigating a particular incident or complaint under investigation -- in the expectation that criminal charges and court process will ultimately be forthcoming -- is generally referred to as "investigative" information. Intelligence information, as we have said, is not related to an investigation of a specific offence. Criminal intelligence information typically relates to the activities and general course of conduct of persons suspected by the police to be involved in criminal activity.

In the OPP, for instance, most detachments maintain a system of reporting information on local criminals, suspects and associates simply in anticipation that the data may prove useful in a future investigation or in detecting and preventing a crime. On a more formal level, most major police forces have intelligence units which collect information about organized criminals of various types and which may advise investigators in specialized units dealing with white collar crime, car theft rings, drug peddling, etc. Information of this kind can be provided to CISO by all police force members and information

is there classified as to its reliability and availability. Some information is merely indexed by CISO in such a way as to indicate that it exists in a given police force.

The OPP Intelligence Branch shares information with other branches in the Special Services Division, such as the Criminal Investigation Branch, the Anti-Rackets Branch, the Security Branch, the Drug Squad, etc., but intelligence files are maintained only within the Intelligence Branch. Strict control on access to these files is maintained. Each member must sign for a file when it is taken out. Within the Branch there are 2,000 master files on prime targets which are usually individuals. These files contain information on associates and organizations involved with an individual; for example, business firms. Names of individuals and organizations in the file are card-indexed for cross-reference purposes. It is estimated that there are now approximately 80,000 names in these files, dating back to the early 1960's.

Most intelligence units use a similar file structure. A long-term historical record of the activities of key individuals is important because these persons sometimes drop out of sight or go abroad for long periods and it is necessary to pick up quickly on their activities when resumed. Even if an individual dies the files are not destroyed because data in the file about associates and organizations still may provide useful information on activities undertaken by the entire group. In addition, such ongoing information is used to advise the Commissioner

of Police, the Premier, ministers and other public figures about persons with whom they deal who may be linked to organized crime. This may be as innocent as, for example, an invitation to a testimonial dinner for an individual who has been found to have links with organized crime. Such association by a key public figure could prove quite embarrassing, and the intelligence unit seeks to prevent such incidents.

Intelligence information is collected mainly from individual contacts by intelligence officers, who guard their sources closely, even amongst themselves. These sources could be informants, other police forces, etc. Investigations usually begin with a tip-off that a deal is being made or that plans are being developed which may lead to a criminal act; it thus becomes important to keep track of the movements of prime targets and their associates. Apart from police sources, informants are not usually named in files, although the information itself might indicate the informant's identity. Information collected may also be used, of course, to clear someone suspected of involvement. The types of cases and investigations carried out by the Intelligence Branch widely, from arson to fraud or extortion.

Police officers working on case investigations may desire information gathered by CISO. These files may be accessed only by the full-time intelligence officers who are CISO members. Thus, it is only through the cooperation of an intelligence officer that an ordinary investigation may benefit from this data. The CISO monitors major investigations

in the province, and it is conceivable that CISO would contribute information from its stores in that context. As indicated earlier, the criminal intelligence network in Canada has recently been computerized. This new computerized system, ACIS, will be described in a subsequent section of this chapter.

CISO maintains a name index which is currently being transferred to a computerized data base. The index contains all names gleaned from intelligence reports and will facilitate access to a full file relating to the individual in question, or to any other file in which the name appears, either stored on ACIS or in document form. We were informed that CISO has under 500 active files, but 60,000 to 70,000 entries in the name index. Each name entry indicates the main file where it appears. The name file thus also acts as a cross-index and may assist in identifying patterns of behaviour of criminal networks. This same data base is used by the OPP to analyze telephone numbers obtained through wiretaps. Cross-referencing of telephone numbers to the name index is possible. Both CISO and OPP Special Services Branch have access to the data base, although either one may enter information in such a way as to preclude the other from accessing it.

Confidentiality of both information and sources is obviously of paramount concern to CISO. This concern is reflected in all aspects of its current policy on the collection, use, storage and dissemination of intelligence information.

b) Political or "Security" Intelligence

The gathering of political or "security" intelligence is undertaken primarily by the Security Branch of the OPP, whose mandate is to assure the security of "government." The latter term is, for these purposes, broadly construed and is taken to include elected members of the legislature in all parties, civil servants, and the agencies and physical property of the province. Unlike other police work which is directed at investigating criminal acts and bringing criminals to justice, the task of the Security Branch is to prevent the occurrence of disruptive activity in order to assure the uninterrupted operation of government. Thus, for example, letters or telephone calls threatening the life of an important public official would be traced, and the originator investigated. Records about these persons are maintained so that if the official were to visit a city in which such an individual resided, precautions could be taken against that person. Similarly, with groups that state their purpose as the violent overthrow of the state, files are kept so that the participants may be identified and their likely activities plotted. Thus, for example, if a demonstration were to be held in which such a group would likely participate, extra police may be put on duty in anticipation of violent activity.

The investigation of persons and groups considered dangerous to the state has been cut back in recent years, in favour of the other major type of work carried out by the Branch -- the conduct of "security

checks." This work provides ongoing internal security as opposed to preventing external threats. Security guards and some highly-placed civil servants must be investigated, before hiring, and this is done by the Security Branch.

Finally, we might note one further type of work undertaken by the Security Branch -- the "sweeping" of government offices to detect surveillance devices in order to thwart improper electronic surveillance of public officials.

At the present time, some of the manually-stored political intelligence data is being transferred to computer storage. It will be retrievable by geographical identifiers, by a description of the type of activity in which the person is likely to engage, and by the individual's name. There is some linkage planned with other police information computers, so that an inquirer on CPIC would "register a hit"¹⁴ and if inquiring about an individual, for example, would learn only that the person in question was on file for security purposes. No further information would be made available routinely to the inquirer.

5. Criminal History Dossiers

Within a police force, the records section serves as its collective

14 A "hit" is a match between a CPIC record and an individual, vehicle or piece of property located by police.

memory, storing information about the criminals, suspects and crimes dealt with by the force over the years. While much of this information is unlikely to be used again, it is nonetheless a potential source of data pertinent to future investigations. In the OPP, the Central Records and Communications Branch holds almost 400,000 files or dossiers on all persons charged with indictable Criminal Code offences. These criminal history files contain all the data gathered by the force about a particular individual. However, files are not kept centrally about individuals who are arrested but later released without being charged.

Files contain such documents as conviction notices, summary conviction tickets or charge sheets, fingerprints, photographs, parole reports, temporary absence permits and even telex messages about the individual, his/her movements and associates -- in fact, any data collected by the force during the course of investigation. In addition, some files may contain information gathered from informants in which these sources are named. Such files are retrieved through a system of index cards which bear the name, age, address plus other identifying information such as fingerprint number about persons in the central files. Current retention policy allows files to be kept until the file subject reaches age 70 or dies.

Most police forces of any significant size maintain a similar system of central criminal records. However, with the advent of the CPIC network, this situation is changing since all forces now have ready access to RCMP criminal history files which duplicate much of the

information held by local forces. The OPP, therefore, has recently decided to abandon its central criminal history file system and to rely on RCMP records. Thus, the only criminal history files to be maintained by the OPP are likely to be local files held by detachments and district headquarters. The central dossier files are to be destroyed by a method as yet undetermined.

An exception to these general practices relating to criminal history files is made for juveniles. The OPP does not retain records about juveniles charged with delinquency under the Juvenile Delinquents Act. There is no statutory prohibition against the police maintaining such records. However, we understand that neither the OPP nor other police forces do retain them. On the other hand, occurrence reports are retained. These contain information about any juvenile involved in a particular incident, and a record of the young person's name appears in the name index.

6. The "Criminal Record"

While the criminal dossier may contain a wide variety of information, some of which may have been received from informants or from casual observation of the individuals by patrolling police officers, the dossier also contains a record -- not necessarily on one piece of paper, however -- of that person's dealings with the police, the courts and possibly correctional institutions. The file would probably contain a

record of arrests, charges, convictions and sentences, most of which would be matters of public record through the courts and the press. This collection of data is generally understood within the law enforcement community to constitute the individual's "criminal record." Although there is no standard definition of this term, it may be that the general public assumes that the "criminal record" is constituted only by convictions and sentences. In fact, however, the broader range of material referred to above is included as part of the "record" which may circulate within the law enforcement community.

The RCMP now acts as a central repository of information of this kind, and provides to law enforcement agencies, on request, a criminal record check. A copy of the formal criminal record maintained by the RCMP may, of course, find its way back into the local criminal history files referred to above. The RCMP response to record check inquiries is provided on a form, on one-half of which is a list of the individual's convictions, their date, location and disposition. On the other half of the form, labelled "for police purposes only," charges are listed which have been dismissed, withdrawn, or for which the accused has been found guilty but has received an absolute or conditional discharge. In addition, there is a listing of the agencies that received copies of the record check. Such information is provided to the RCMP by all police forces, courts and correctional institutions, and is updated as data on the status of a charge comes in. For example, if a correctional institution requested a fingerprint check on a new inmate for identification purposes, the RCMP would respond by requesting details of

the conviction and sentence, in order to verify information likely to have been received from the court.

In addition, the criminal record contains other identifying information in a separate document. The most important information of this type, where available, is a set of fingerprints -- the most reliable means by which a record can be identified to an individual. Names and addresses are not unique to an individual, and birthdate is often inaccurately given. Where criminal records contain a set of fingerprints, the record is identified by a fingerprint number, which is then used as a common identifier within the criminal justice system.

At one time, the OPP carried out criminal record checks itself, but due to difficulties in coordinating all the necessary data and since the RCMP already had all this data, the OPP now refers all inquiries to the RCMP.

Of particular interest from a privacy protection perspective, of course, is the possibility of removal or destruction of items in the "criminal record." First, individuals may be concerned to retrieve their fingerprints, particularly in cases where charges against the person have been withdrawn or dismissed. On this point, it should be noted that there is no legal requirement for the return or destruction of fingerprints or photographs following withdrawal or dismissal of charges. However, the OPP's policy is to return such documents, on request, where the individual has no previous record. In cases where it would

not be "in the public interest" to do so, such a request would be denied.

With respect to the criminal record in a more general sense, the federal Criminal Records Act,¹⁵ which provides for the granting of pardons by the federal government, is of particular relevance. Under the Act, any person convicted or found guilty of an offence under an Act of Parliament of Canada or a regulation thereunder may apply for a pardon to the Solicitor General of Canada.¹⁶ After an investigation into the applicant's behaviour (which does not take place until one year after a discharge has been granted, or until two years after the completion of a sentence for a summary conviction offence, and until five years for other offences), the minister may recommend to the Governor in Council that a pardon be granted. The effect of a pardon is that the minister may order judicial records to be delivered into the custody of the Commissioner of the RCMP, and then bar its further use or disclosure. Any record of a conviction in respect of which a pardon is granted -- within the custody of the RCMP or any other federal department or agency -- must be kept separate from other criminal records. The fact of the existence of the record or of a particular conviction must not be disclosed. The Act also provides for the revocation of a pardon if the person concerned is subsequently convicted of a further offence, or is otherwise found to be of

15 Criminal Records Act, S.C. 1969-70, c. 40. See also provincial legislation to this effect, Summary Offences Relief Act, S.N.S. 1970, c. 18.

16 Ibid., s. 3.

unacceptable conduct. In effect, then, the Act does not provide for the expunging or destroying of criminal records, but only that they be sealed from dissemination and use.¹⁷

Even though the Criminal Records Act applies only to federal government agencies, the OPP does comply with the spirit of that law. On notification of a pardon, the practice of the OPP is to remove the record from the general criminal history files and place it in a locked cabinet. Similar practice is reported by municipal forces.

Apart from full criminal record checks of the kind described above, a brief criminal record synopsis is available to police forces directly from the CPIC computer data bank. Eleven categories of offence are available to respond to inquiries. A response would indicate, for example, that John Doe has been charged or convicted for theft, fraud and assault. There would be no indication of the total number of offences in any category nor the exact nature of an offence, nor would there be an indication of which charges resulted in convictions. The purpose of the response is simply to indicate to police agencies that a record of involvement with the criminal justice system exists and to indicate the kind of offence. An inquiry to CPIC may give the record for several different John Doe's, although the inquiring police officer would try to reduce the possibility of this occurring by providing the address, date of birth, and any other identifying information to the

17 Ibid., s. 6(2).

computer. If further information is desired, an inquiry would then be made to the RCMP for the complete criminal record. If the laying of a charge is contemplated, the record is checked against the fingerprints of the person to be charged so as to ensure an accurate identification. The sensitivity of criminal record information and the need for complete accuracy is obvious. The RCMP continually check with police forces, courts and correctional institutions as to the disposition of convictions reported to them.

Under the provisions of the Canadian Human Rights Act, Part IV,¹⁸ it is possible for a person to obtain a copy of his/her criminal record held by the RCMP, although exemptions from access may be invoked for criminal history support documents. To obtain a copy of the criminal record, a person is required to provide a complete set of fingerprints taken by an accredited law enforcement agency. In the case of the OPP (which is not covered by the Canadian Human Rights Act), few such requests have been received. If this does happen, however, the force requires the individual's full name and birthdate before it makes a check of RCMP records, which can be done through the CPIC communications network. If a record exists for a person of that name and age, the individual is informed of this, but is not informed about where the offence occurred. Should the individual then wish to obtain a complete record, s/he must provide a set of fingerprints so that a positive identification with the prints included in the RCMP-held record can be made. The fingerprints taken for the check are returned to the individual.

18 S.C. 1976-77, c. 30.

E. The Computerization of
Law Enforcement Information Systems

As in other information contexts, the use of computers increases the capacity of our information systems to meet the needs of its users. In a geographically vast country like Canada, coordination of law enforcement information which would otherwise be impossible can be achieved through computerized networks. We have indicated in another chapter of this report, however, that there are a number of privacy protection problems inherent in the use of computers.¹⁹ For example, the need to reduce detailed information, sometimes based on opinion rather than fact, to coded factors which may be entered in the computer program may reduce the accuracy of the information. Moreover, the maintenance of accurate data is dependent on thorough and consistent practices for updating computerized files. In this respect, it is disturbing to note that a recent study of computerized criminal justice records in New York State indicated that only 27% of the files were accurate and complete.²⁰

Ontario police forces have begun to use computerized information systems both locally and in connection with larger networks. As mentioned previously, two computerized systems are now in use on a national basis in Canada: CPIC -- the Canadian Police Information Centre, and ACIS -- the Automated Criminal Intelligence System. We will describe each system

19 See Chapter IV.

20 "U.S. study finds most records err," Globe and Mail, March 6, 1977, 5.

briefly in turn.

1. CPIC

CPIC came into use in 1972. This system stores operational police information which is required to support police services across Canada. It is operated by the RCMP on behalf of all police forces in Canada. Essentially, it is a large computerized information bank which serves as an index to information held by individual police forces.²¹

The type of information CPIC holds is concerned with day-to-day police operations -- wanted or missing persons, stolen vehicles, stolen property and firearms. A criminal record index is also included on the system. All Ontario police forces which provide 24-hour round-the-clock service are linked to the CPIC computer through a communication network and 253 remote terminals. The network is also used for teletype communications between individual police forces. All information on CPIC (except the criminal record index) originates with a police agency which is responsible for updating, correcting or removing the information it has placed on the system. No police force may alter information provided by another force.

21 See generally, "Canadian Police Information Centre," RCMP Publication 7610-21-876-3477.

The major types of information placed on CPIC concern persons, vehicles and property. Information about persons covers those wanted (on a warrant), missing or on parole, and those prohibited from driving motor vehicles or from possessing firearms or liquor. In addition, police forces may include remarks about individuals who, for example, are known to be dangerous.

As indicated previously in this chapter, the RCMP makes available through CPIC a criminal record synopsis which summarizes criminal offences and charges into 11 categories of crime. This serves in effect as an index to the full criminal record held by the RCMP.

Information relating to Ontario drivers is also stored on CPIC. Indeed, the use of CPIC in this respect illustrates the enhanced capacity of law enforcement information systems effected through the use of the computer. Drivers convicted of driving offences may be suspended from driving by court order. In all cases, the suspension, administered by the Registrar of Motor Vehicles at the Ministry of Transportation and Communications, is noted on the drivers files maintained by the Registrar. However, prior to CPIC, there was no effective method of enforcing suspensions inasmuch as police officers could not readily identify drivers who were suspended. Consequently, it is believed that many persons chose to ignore suspensions. The penalty for so doing was relatively ineffective. In 1975, a program was initiated by the Ontario Police Commission and the OPP to place the names of suspended drivers on CPIC. As a result, a police officer may now make a roadside check

over the radio to determine whether a particular individual is driving under suspension, and may also confirm with the Driver Suspension Centre that such CPIC-held information is correct. Since the program was introduced, it has been estimated that the enforcement of suspensions has doubled.

Another interesting development is the linking of the CPIC communications network with the computerized files of both drivers and registered motor vehicles in Ontario. The MTC vehicle file data bank has been directly linked to the CPIC data bank by means of telecommunications through which police forces may obtain desired vehicle information about any vehicle registered in Ontario. The driver file is now linked to the CPIC network in a similar fashion. Traditionally, the police have extensively used driver and vehicle information to identify individuals involved in crimes as well as to enforce traffic laws. Developments to improve police accessibility to these files resulted from problems caused by delays in updating vehicle ownership and licence registration information. Although updating problems have not been resolved in the Ministry of Transportation and Communications record-keeping system (see Chapter XV), at least the police now obtain approximately the same currency of data as is held by the MTC. With these linkage facilities in place, the amount of police work currently required to enforce suspensions and warrants may reduce considerably. Payment of fines could be required before vehicle registration is renewed.

Overall policy on the use of CPIC is determined by the CPIC Advisory Committee. All major police forces in Canada and the Ontario Police

Commission are represented on the Committee. Use of the system by Ontario police forces is controlled by the Ontario Police Commission. Ontario has used its discretion to impose stricter rules than those established by the Advisory Committee regarding the system's operation, but it may not relax the Advisory Committee's rules.

Under a federal-provincial agreement signed by the Ministers of Justice in 1972, Ontario pays for half of the communications lines and terminals and controls the number of terminals used in the province. Each province determines which police forces may use CPIC. In Ontario, only the Ontario Police Commission, the Centre of Forensic Sciences and the Coroner's Office have CPIC terminals.

The policy regarding confidentiality and protection of information on CPIC makes each agency with direct terminal access to CPIC files responsible for the confidentiality and dissemination of information placed on or retrieved from the system. Every piece of data on the system is identified with the originating police force. When requested information is transmitted by the computer, the message concludes with the statement "Confirm all hits with originating agency." This suggestion that direct contact be made with the force holding the original data reflects the fact that the CPIC file is regarded only as an index to information held by local forces. By checking the detail and accuracy of the CPIC information with its original supplier, an attempt is made to ensure that actions are not taken on the basis of erroneous data. Notwithstanding this policy, however, it would be

wrong to think of CPIC as merely an index of data which itself does not form the basis of decisions affecting the individual. Police may, for example, hold an individual suspected of being wanted on an outstanding warrant on the basis of a CPIC message while confirmation is obtained. CPIC is thus not just an index of information. It is an important and increasingly powerful tool for operational law enforcement.

The need to protect against police use of erroneous or out-of-date information on CPIC to make decisions is well-recognized, and forces are continually reminded of this by both the RCMP and the Ontario Police Commission. The latter continually carries out an audit of CPIC use by Ontario police forces. Each force is completely audited once every two years. Every record entered by the force currently held on CPIC is checked to ensure that the force holds the correct documentation in its local files. Few instances of records from CPIC being released outside police agencies have been reported. We are advised that it is stressed continually within the law enforcement community that CPIC is for the use only of police forces. The ultimate sanction against a police force for breaking CPIC rules is that the force may be cut off from the system.

Finally, we should note that a further extension of the use of sophisticated communications technology is at the point of implementation. Miniature computer terminals enabling police officers to directly obtain limited information from CPIC have now

been placed in selected patrol cars. The ability of police officers to utilize CPIC to obtain driver and vehicle information and other law enforcement system data is obviously much enhanced by this development. Direct communications links of this kind with police vehicles will also be of assistance in assigning and deploying police cars and in providing management information to the police administration.

2. ACIS

ACIS, the Automated Criminal Intelligence Service, is a more recent development in use of computerized information systems by law enforcement agencies. It is a computerized intelligence communications network administered by the Criminal Intelligence Service for Canada — CISC, the coordinating body for nine provincial intelligence bureaus described earlier in this chapter.

ACIS contains reports contributed by member bureaus. In Ontario, the information is processed by CISO staff. CISO, in turn, merely collates and distributes information supplied by its members. Requests to the ACIS system from Ontario must come from CISO members. Disclosures of information to affiliate members of CISO are subject to the rules of confidentiality described in an earlier part of this chapter.

Information obtained by a CISO member may be disclosed, at the member's discretion, to an ordinary investigating officer for use in a specific investigation.

The information placed on the system is retrievable on the basis of various personal identifiers, the individual's physical features, the geographical location or crime category. The entry concerning an individual identifies categories of criminal activity, and may contain any of 48 different types of descriptive data including the data subject's criminal history.

A yearly audit is performed on ACIS to assure data currency and relevance. Although the system has not been in operation for very long at the time of writing, plans exist for ACIS files to be retained for only five years unless there is an ongoing interest in the subject. Often, of course, given the nature of intelligence work, there is such an interest in a particular file. In any event, the manually-stored "backup" files are retained even though the ACIS entry may have been destroyed.

The ACIS network is directly linked to CPIC. If an inquiry is made to CPIC about a person listed in ACIS, the ACIS operator receives a signal to indicate this. The ACIS operator may inquire further to determine the location of an individual. ACIS is "blind" to the CPIC system in the sense that the officer who queries CPIC does not learn that the subject of inquiry is on ACIS files unless the ACIS operator relays this information.

The development of the ACIS system has substantially increased the capacity of those agencies and individuals engaged in intelligence work

to effectively share and utilize intelligence information. The speed with which intelligence information can be accessed has been dramatically increased through the use of computers. The ACIS system obviously enhances the capacity of the police to engage in surveillance of any individual whose activities involve numerous locations. Further, the ability to bring intelligence information from a broad range of sources to bear on the analysis of the activities of a particular individual or group of individuals may be especially useful in the context of efforts to monitor and curtail the activities of "organized crime."

F. Access to Law Enforcement Information

Having described in the previous section of this chapter the general nature of law enforcement records and information systems currently in use in Ontario, we turn now to consider a question of obvious relevance to the privacy protection issue -- the extent to which access to law enforcement information is granted beyond the confines of the law enforcement community. Of particular interest in this regard is the extent to which criminal record information is made available, on request, to individuals or institutions which may have an interest in such material.²² Criminal record information is, in theory at least,

22 We have reviewed above the ability of an individual, exercising rights conferred by the Canadian Human Rights Act, to gain access to his/her own criminal record. In this section we are concerned only with the question of access by third parties.

part of the public record in the sense that it is contained in the records generated by the court system in its disposition of criminal prosecutions. Secret trials are anathema in a free society and for this reason, presumably, criminal prosecutions and the resulting court records are, as a general rule, open to public scrutiny. The "criminal record" of an individual is thus contained in these public records, but for all practical purposes it is in reality inaccessible. Court records are not centrally collated or stored and are thus unavailable to the public in a digestible form. The advent of the centralized criminal record system operated by the RCMP thus creates an information resource, albeit consisting largely of information which has never been "secret" as a matter of law or policy in the past, which is capable of permitting new and possibly privacy invasive uses of criminal record information.

The extent to which it is sound public policy either to facilitate public access to criminal records or, on the other hand, to restrict public access to such information so as to permit individuals with a history of criminal conduct to make a "fresh start," is a matter for debate. Our own view is that the public interest in encouraging and facilitating the "fresh start" should, as a general rule, prevail. What cannot be doubted, however, is that the character of these records are dramatically altered once they are collected and collated in a central location.

In our discussions with OPP and local police personnel, it was evident

that the need to protect the confidentiality of criminal record information and the danger from a personal privacy perspective of disseminating such information were recognized as matters of great concern.

Requests for criminal record checks are forwarded to the RCMP by the OPP central records department only in response to requests from Ontario government agencies which have been approved by the Commissioner of the OPP. Most of these agencies have a statutory basis for seeking such information as part of a licensing scheme which explicitly makes "past conduct" a relevant criterion to be considered in deciding whether or not to grant the applicant the licence in question. Over half the checks undertaken by the OPP are made on behalf of the Ministry of Consumer and Commercial Relations, which has a broad range of licensing responsibilities. Other checks are undertaken for ministries which employ investigators or personnel with peace officer status, such as conservation officers in the employ of the Ministry of Natural Resources. In such cases, the individual is specifically asked on the application form whether or not s/he has been convicted of a criminal offence. In response to criminal record check inquiries, the OPP releases only conviction data. If the record returned by the RCMP indicates an arrest but no prosecution, or a prosecution and acquittal, the OPP responds to the inquiring ministry that there is no record. No criminal record checks are undertaken by the OPP for private sector employers or for agencies not approved by the Commissioner, although requests from such sources are continually received.

Local OPP detachments also receive occasional requests for criminal record information. In one detachment we visited, checks are made on behalf of the local Children's Aid Society regarding applicants to become foster parents. In all cases, we were advised that an individual's written approval is sought before a check is made.

As far as local police forces are concerned, a survey of ten municipal police forces indicates that policies governing public access to criminal records vary from one force to the next. Our survey included large regional forces and some small city forces. Some reported requests from a wide variety of organizations seeking criminal record information -- including retail stores, private security agencies, municipal licensing authorities, social agencies and of course other police forces and agencies involved in the administration of justice, including those involved in the supervision of offenders on probation and parole. The range of organizations which in fact are granted access to criminal record information varies considerably from one force to the next. Some forces provide such information only to other police forces. Others also provide information to Children's Aid Societies, Big Brothers and local licensing authorities as well as criminal justice agencies such as the John Howard Society. Only one force indicated that it would provide information to employers with respect to a job application, and then only if the applicant was aware that such a check would be made.

The nature of the information provided also varied considerably. Some forces provide a complete set of convictions. Others only advise whether a record is serious or not serious, although the basis for this judgment was not made clear to us.

The conclusion we reached from this small survey was that although policies vary considerably, the authorized release of criminal record information to non-police agencies is limited. However, recent incidents reported in the press²³ indicate that criminal record information may be passed on to private companies in contravention of policy. This is most likely to occur in situations where, for example, a private investigator who is an ex-police officer has maintained contact with his/her former colleagues.

There is no statutory prohibition on the release of criminal record data by Ontario police forces, except insofar as police discipline procedures under regulation of the Police Act may be used to impose penalties for infractions of the internal policies of police forces.

In order to gain some understanding of the perceived need for such information by private industry, we spoke to representatives of major financial and retail companies. In many cases, applicants for positions were asked on the application form whether they had been convicted of a criminal offence. However, in no instances were we told that attempts had been made to verify such information. Indeed, the individuals we

23 Herman, Wendy, "Phone call opened police criminal files," Toronto Star, article on York-Durham page, summer, 1978.

interviewed in personnel offices did not appear to know how to do so. Members of the security staff of these organizations, however, indicated to us that criminal record information might be obtained when cooperating with a local police force in the investigation of a specific offence. Since most senior security officers have had prior police experience, it is not surprising, as suggested above, that their network of information could give them easier access to criminal record data than other employees. Nonetheless, it appears that routine checking of job applications would rarely occur, since it would depend on continuous and relatively frequent access to police records. Such access is more likely to arise in the course of specific investigations by security staff.

Local agencies dealing with children, such as Children's Aid Societies, have a compelling claim for access to criminal record information when assessing applicants as volunteers or foster parents. A concern expressed to us by the police with respect to providing information to such agencies is that control of the data would pass out of police hands, and its confidentiality could therefore no longer be guaranteed. Arrangements for record checks are thus usually made on an individual basis between each local agency and police force. In all of the cases drawn to our attention, we were advised that the approval of an individual is sought before the police record check is made. The agency is then notified whether a record does or does not exist and if there is a record, only the nature of the offence is disclosed. In most instances, agencies tend to ignore an old record, but practices vary. A

record of a sexual offence, however long ago it might have been committed, usually results in the rejection of an applicant "if only," as one interviewee stated, "from the point of view of public credibility."

G. Discussion and Conclusions

We turn now to a consideration of some of the privacy protection issues which arise from the collection and use of personal information by law enforcement authorities. In many respects, our investigation of these matters must be considered to be a preliminary inquiry. As we have indicated, it was not our mandate to enter into an exhaustive examination of all of the privacy protection issues relating to the activities of law enforcement authorities. Moreover, it is inherent in the nature of the empirical work which we were permitted to undertake that we cannot purport to have given a full and completely accurate account of that which has been the focus of inquiry -- law enforcement information systems. Nonetheless, we feel that the results of our research do provide a basis for informed consideration of a number of privacy related issues.

1. The Collection of Intelligence Information

First, we have noted the extensive collection of criminal intelligence information and information which we have described as political or

"security" intelligence by law enforcement authorities in Ontario. Although we would not deny the utility of such information for valid law enforcement purposes, it is evident that a number of privacy concerns relating to surveillance activity of this kind should be addressed in the formulation of a privacy protection policy for Ontario.

In our view, legitimate concerns may arise with respect to the scope of intelligence gathering. We note that the subjects of such surveillance may be individuals who have never been convicted, or indeed accused of any criminal act. The names of persons who have merely had innocent contact with others with such a background may appear in intelligence files and in the computerized name file which we have described. The broad range of potential sources of such information -- both foreign and domestic, many of them potentially unreliable -- and the unverifiable nature of some of the information which may find its way into the system gives rise to classic informational privacy problems and suggests that the scope of such surveillance should be carefully limited to cases where a clear need for it can be demonstrated.

These concerns are especially intense with respect to the gathering of political intelligence information. Difficult lines must be drawn between surveillance of individuals who are indeed prone to committing acts of political violence and subversion and those who pose no such threat and are merely exercising democratic rights of dissent. In our view, it is important not only that such distinctions be carefully and sensibly drawn, but also that they be drawn in such a fashion that the

public will have confidence that proper limitations on such surveillance activity are being observed by the security services.

For these reasons, we believe that it would be in the public interest to adopt a clear statutory standard for the scope of intelligence gathering activity. In particular, we endorse the standard proposed by K.P. O'Connor in a research publication of the Australian Law Reform Commission²⁴ in the following terms:

Personal information should only be collected or held where it is relevant to the purpose of the collection. Convincing reasons should exist to justify the collection of highly sensitive personal information. In particular, an individually identified intelligence record should not be maintained about the activities, associations or beliefs of an individual about whom there is no reasonable ground to suspect involvement or participation in criminal activity.

A similar standard has been adopted in legislation in Iowa, which prohibits the maintenance by either manual or automated means of any "surveillance data," i.e.,

... information on individuals pertaining to participation in organizations, groups, meetings, or assemblies where there are no reasonable grounds to suspect involvement or participation in criminal activity by any person. 25
(emphasis added)

Regardless of whether a standard of this kind is to be embodied in statutory form, we feel that public confidence in the fairness of

24 K.P. O'Connor, Federal Police Records, op. cit., 47.

25 Iowa Code, c. 692 (1974) s. 9.

intelligence gathering and its consistency with fundamental democratic values would be much enhanced by the establishment of an independent power of inspection and comment in a respected public official. We note here the experience of the Privacy Committee of New South Wales. The powers of this Committee to engage in inspection and reporting activities have been described elsewhere in this report.²⁶ In 1978, the Committee undertook an examination at the request of the Premier of New South Wales, of the security or intelligence files maintained by the New South Wales Special Branch, a rough equivalent to the OPP Security Branch. The Committee reported in its findings that much of the file material was both privacy invasive and unnecessary to legitimate security needs.²⁷ Three months later, the Premier announced that 50,000 of the 80,000 files held by the Special Branch had been destroyed.

We believe it would be in the interest of the security services and of the public at large to ensure that an independent vetting of intelligence information gathering activity can occur on a regular and routine basis. The security services would benefit from clearer guidance as to the proper scope of this activity and from renewed public confidence in the legitimacy of their work. The public would benefit, we believe, from the reduction of anxiety concerning the nature and scope of intelligence work and the development of a

26 See Chapter VI.

27 See O'Connor, op. cit., 23.

well-founded belief that an appropriate balance is being struck between the need for intelligence gathering and the need to ensure that important values of democratic freedom and personal privacy are not unduly sacrificed to these objectives.

Similar views have been expressed by the U.K. Data Protection Committee in rejecting the idea that intelligence information systems should be exempt from the supervision of the proposed Data Protection Authority. The Committee stated

If the job [of intelligence gathering] is to be done properly, it must necessarily be done in secret. If that is so, it can never come under public scrutiny ... This leaves the security services in a hermetic compartment where they can never discuss their problems with anyone outside their own tight community; thus they are not open to the healthy -- and often constructive -- criticism and debate which assures for many other public servants that they will not stray beyond their allotted functions. 28

The Committee recommended that a senior official with security clearance be appointed to the DPA, to ensure that due regard is paid to the protection of privacy in this area. In Sweden and France, similar powers of inspection have been assigned to a public official.

2. Disclosure of Law Enforcement Information to Third Parties

Our survey of law enforcement information practices has provided two

28 Report of the Committee on Data Protection (Lindop Committee), (Cmd. 7341, 1978) 222.

examples of the disclosure of law enforcement or intelligence information to third parties: criminal record checks and security checks. The disclosure of information for these purposes raises informational privacy concerns which appear, for the most part, to be addressed in current practice.

With respect to criminal record checks, it is commonly the practice of police forces in Ontario to undertake such checks only where the data subject has consented to an investigation of this kind. This is not, strictly speaking, true in cases where criminal record checks are undertaken on behalf of ministries of the Ontario government engaged in the review of applications for licences of various kinds. Typically, the application form instructs the applicant to reveal his/her criminal record. The application forms which we have reviewed do not indicate further that inquiries will be undertaken on behalf of the ministry to the RCMP criminal records data base in Ottawa. We see no reason why application forms should not indicate that such inquiries (and indeed any other kinds of investigation) will be undertaken.

More generally, it is our view that the general practice followed in the province to the effect that criminal record checks are only undertaken with the consent of the data subject ought to be uniformly adhered to by all law enforcement agencies. Similar questions arise with respect to the undertaking of security checks. We understand that the normal procedure is to advise the potential subject of such a check that a security investigation will be undertaken by the OPP.

One final point concerning access to law enforcement information by third parties must be considered. The third party requestor will normally seek access for the purpose of making a decision of some kind relating to the data subject. It is thus important that the data subject have an opportunity to ensure that the information which the third party receives is accurate. This should not pose any difficulty with criminal records. As they are available to the data subject from the RCMP, there should be no objection to allowing the data subject to ensure that the third party has received an accurate copy of the record. Security checks, however, give rise to a difficulty which is not found in the context of criminal records. Security checks will likely contain information which law enforcement officials will not want disclosed to the data subject. It is possible, then, that the data subject may, for example, be deprived of an important job opportunity on the basis of information which cannot be confirmed or vetted by the data subject. The proper resolution of this difficulty, we believe, is to require that the substance of the material allegations made in the file be communicated in such a way as to avoid compromising intelligence gathering activity but to permit an informed response by the data subject in an attempt to correct erroneous allegations in the file. Determination of the proper level of disclosure in such instances should be confided to a public official whose powers would include the right to inspect the file.

A similar proposal has been put forward by K.P. O'Connor in the Australian Law Reform Commission research publication referred

to above.²⁹ We will return to this point below in the context of our discussion of the general problem of data subject access to law enforcement files.

3. Subject Access to
Law Enforcement Information

As we have indicated elsewhere in this report, one of the principle mechanisms for ensuring that fair information practices are adopted by agencies which gather and use personal information is to provide the data subject with the right to have access to files containing personal information. In other chapters of this report, we have indicated our opinion as to the manner in which this principle can be adopted in the various information contexts which form the subject matter of our case studies. Without doubt, however, law enforcement information systems provide the most difficult context in which to implement this principle. Obviously, there is a very compelling interest, as far as the individual is concerned, in learning as much as possible about the contents of law enforcement information systems which concern him/her. On the other hand, there are undeniably compelling interests in secrecy with respect to such files in order to facilitate effective law enforcement activity.

29 O'Connor, op. cit., 57-58.

One solution to this dilemma, of course, would be simply to exempt all investigative and intelligence law enforcement information from the general principle of subject access. We do not favour such a solution, however, for the reason that it fails to give adequate recognition to the importance of permitting subject access to personal files, wherever possible, as a device for ensuring the recognition of the importance of privacy protection considerations.

A better approach, we feel, would be to draft exemptions from the general principle of subject access which would adequately protect the need of enforcement authorities for secrecy with respect to such matters as the identity of informants, law enforcement techniques, and information contained in files related to active investigations. Having thus assured that the law enforcement agencies have adequate protection of their information gathering activities, a citizen would then be assured that any personal information falling outside this range of protected interests would be accessible to him/her.

Useful illustrations of the type of exemption which could be drafted are represented in the American freedom of information legislation and in the proposals for a freedom of information law recently put forward in Australia. The American statute, for example, provides the following exemption to the general principle of openness in government records for the purpose of protecting law enforcement information:

[I]nvestigatory records compiled for law enforcement purposes, but only to the extent that the production of such records would (A) interfere with enforcement proceedings, (B) deprive a person of a right to a fair trial or an impartial adjudication,

(C) constitute an unwarranted invasion of personal privacy, (D) disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source, (E) disclose investigative techniques and procedures, or (F) endanger the life or physical safety 30 of law enforcement personnel.

A more detailed proposal for a provision of this kind was put forward in a Minority Report to the Report of the Royal Commission on Australian Government Administration. The proposed law enforcement exemption is the following:

35. (1) An agency may refuse to disclose a document the disclosure of which could have a substantial adverse impact on enforcement of the law, but only to the extent that disclosure could be reasonably expected to:

- (a) interfere with an enforcement proceeding;
- (b) interfere with an investigation undertaken with a view to an enforcement proceeding or from which an enforcement proceeding might be reasonably expected to eventuate;
- (c) reveal investigative techniques and procedures currently in use or likely to be used;
- (d) disclose the identity of a confidential source of information, or disclose information furnished only by that confidential source;
- (e) endanger the life or physical safety of a law enforcement officer;
- (f) deprive a person of a fair trial; or
- (g) constitute an unwarranted invasion of privacy.

(2) Sub-section (1) shall be read, so far as possible, so as not to include a document of the following, or of a similar nature, namely:

- (a) a document revealing that the scope of any law enforcement investigation has exceeded the limits imposed by law;
 - (b) a document revealing the use of illegal law enforcement techniques or procedures;
 - (c) a document containing any general outline of the structure and programs of a law enforcement agency;
 - (d) a report on the degree of success achieved in a law enforcement program or programs, including statistical analysis;
 - (e) a report prepared in the course of routine law enforcement inspections or investigations by an agency which has the function of enforcing and regulating compliance with a particular law other than the criminal law; and
 - (f) a report on a law enforcement investigation, where the substance of the report has been disclosed to the person who, or the body which, was the subject of the investigation.
- 31

The Australian draft purports to take advantage of some of the principles developed in the American case law interpreting the federal American freedom of information law. We would agree that it might be wise to include a more complete statement of the law enforcement interests as is provided in the Australian model.

There are two concerns, however, which lead us to put forward an additional recommendation concerning personal information which would be exempt from access under an exemption along the lines suggested above. First, we note that in certain cases, exempt information may provide the

31 Report, Royal Commission on Australian Government Administration, (1976) Appendix Vol. 2, 45.

basis for government action relating to an individual. As we have indicated above, such is the case with security checks. Information which would form the basis for a decision not to employ a particular individual would probably be exempt from access by that individual under the scheme proposed above. We feel that it is essential therefore, that an independent party such as a privacy commissioner should have a right of access to such files in order to ensure that some mechanism is in place for protecting the privacy of an individual. The independent authority ought not, in our view, have the power to give access to exempt documents to the data subject, but should have the ability to comment on the nature of the information contained in the file, to make recommendations with respect to the file on behalf of the data subject, and as we have suggested above, to indicate the substance or nature of allegations in the file which may form the basis of a decision, for example, to deprive the data subject of a licence or an employment opportunity.

Our second concern reflects our earlier discussion concerning the delineation of the proper scope of intelligence gathering activity. If intelligence information is to be generally exempt from the principle of subject access, we feel this provides a further and compelling reason for the establishment of an independent authority with powers of inspection and comment with respect to intelligence gathering activity. Regarding the particular problem of subject access, it would be appropriate to allow the independent authority to review the question of whether a particular item of information is truly exempt, and where

it is not, to order disclosure of the information in question to the data subject.

4. The Gathering of Law Enforcement Information
from Private and Public Institutions

As we have indicated above, our study has not yielded much information with respect to the obtaining of personal information by law enforcement authorities from public and private institutions such as government ministries and agencies, banks, credit unions, insurance companies, telephone and credit companies, and hospitals. One interviewee did indicate that such sources were frequently used by the police. Yet, we have no clear understanding of the extent of such use or its value to law enforcement authorities.

As we have noted, the question of law enforcement access to information in the hands of private institutions has been the subject of extensive investigation by the American Privacy Protection Study Commission.³² The philosophy adopted by the Commission in fashioning its recommendations, in essence, was that information which the data subject would expect to be treated confidentially by the private institution in question should be subject to the same protections as have been traditionally accorded to the individual with respect to the

32 U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society, op.cit., 41-486.

privacy of one's home environment. Thus, the Commission recommended that access to such personal data should be obtained from private institutions only under the authority of a properly issued warrant or other judicial order. We are in agreement with these views. Similar rules should apply, we feel, with respect to the granting of police access to personal files maintained by government institutions.

5. Computerization of
Law Enforcement Information Systems

As we have seen, the last few years have witnessed an extensive implementation of sophisticated computer technology by the law enforcement community. We indicate elsewhere in this report that the computerization of personal information systems is a process giving rise to a number of privacy concerns, and as our account of this process indicates, a number of such concerns have obviously played a role in the design and implementation of the CPIC and ACIS systems.

We do note, however, that the computerization of law enforcement systems is a subject which has given rise to considerable uneasiness in other jurisdictions. Thus, for example, the recent report of the British Data Protection Committee entered the following caveat concerning the establishment of computerized law enforcement information networks:

We think it is important that the confidence and respect which, by and large, the public in our free society still

has for police is to be preserved, that major policy decisions about computerized policy applications handling personal information should not be taken in secret. 33

It is obviously rather late to offer similar advice with respect to the implementation of such systems in Ontario. Nonetheless, we do believe that it is not too late to suggest that the operation of such systems and the proposals made, from time to time, for their alteration or extension should be subject to examination and comment by a body whose mandate it is to articulate and discuss the privacy protection implications of government personal information handling practices. The establishment of new systems and the linkage of existing systems are both matters which could usefully be scrutinized in this way.

33 Report of the Committee on Data Protection (Lindop Committee),
(Cmd. 7341, 1978) 221.

CHAPTER XIII

CORRECTIONS, PROBATION AND PAROLE

The Ministry of Correctional Services is responsible for administering all adult correctional institutions and jails in the province and adult probation and parole programs. In general, the Ministry deals with offenders sentenced to terms of less than two years, although those sentenced to longer terms and therefore destined for federal institutions pass through the Ministry's hands at some point.

Four types of correctional institutions are maintained for adults by the province. Jails and detention centres provide maximum security to house individuals who are either awaiting trial or sentencing, being held for immigration hearings or for deportation, awaiting transfer to federal institutions or are serving very short sentences. Correctional centres operate under both maximum and medium security conditions, and offer supervised industrial and work programs. Adult training centres offer programs approved by the Ministry of Education. Treatment facilities deal with inmates suffering certain psychiatric problems.¹ In total, there are 48 such institutions in the province.

1 Ontario Ministry of Correctional Services, Annual Report (Toronto, 1979) 19.

In addition to terms of incarceration in these institutions, the Ministry supervises convicted persons on parole and on probation. Parole is a means of releasing an offender into the community under supervision while s/he serves the remaining portion of incarceration.² There are parole boards at both the federal and provincial levels, but it is the Ontario Board of Parole which makes parole decisions for all inmates in provincial institutions.³ Probation is the sentencing disposition of a court authorizing an offender to be at liberty in the community subject to conditions prescribed in a probation order or a community service order. Generally, these conditions require the person to be of good behaviour and to report to a probation officer at fixed intervals. Other common terms include not consorting with known criminals, not using drugs or alcohol, not carrying firearms and not leaving the jurisdiction.

For the year ending March 31, 1978 there were 61,834 admissions to detention centres and jails. Of these, 38,509 resulted in sentences to terms of imprisonment. A total of 14,387 persons were in custody in correctional centres during the year ended March 31, 1979, of whom 2,885 were already in custody on April 1, 1978 and 2,734 remained on

2 Ibid., 9.

3 Prior to August 1, 1978 persons serving indeterminate or indefinite sentences in provincial institutions were subject to the jurisdiction of the National Parole Board. The Criminal Law Amendment Act, 1977 abolished indefinite sentences, and as a result the provincial Board assumed responsibility for parole decisions about all inmates in provincial institutions.

March 31, 1979. In considering how many personal files result from this population, note that a person may be admitted more than once a year, which means more than one file may be developed.

A total of 64,477 persons were under mandatory supervision during the year ending March 31, 1979, of whom 39,984 were placed there during the year. Parole applications totalled 5,440 for the year, and 1,968 persons were granted parole.

These figures give an indication of the large numbers of people dealt with by the Ministry. It should be pointed out, however, that the majority are held by the Ministry for only short periods pending payment of a fine, release on bail, or the serving of a brief term of incarceration. In such cases, the amount of personal information collected by the Ministry, although extensive, is generally limited to biographical details. However, when a person serves a longer sentence, a more searching examination may be made which may include a psychiatric assessment and a routine reporting of his/her behaviour and attitude. Similarly, a person placed on probation or parole is subject to the watchful eye of a probation officer or the parole board and is liable to be reported on in greater detail.

In our examination of personal records kept by the Ministry, we therefore concentrated on those records containing the most sensitive information to determine how they are maintained and the problems which might arise if access to them was granted.

As in law enforcement, the main misgivings held by correctional services, probation and parole administrators about providing inmates with access to their files and the right of correction concern the adequate protection of the confidentiality of sources of information, and the related problem whereby important information may no longer be given, particularly information about an inmate's personality, behaviour and background. In order to assess the validity of these concerns and to suggest possible alternative measures to ensure privacy protection in the field of corrections, we examined in some detail the kinds of records kept about inmates and parolees and the way in which information is collected and disseminated.

We visited the head office of the Ministry of Correctional Services to see how the adult information system and inmate record system works. We also examined records maintained by the Ontario Board of Parole. We visited a correctional institution to examine the records typically kept in that type of facility. We spoke to probation workers and in addition we had the opportunity to attend a workshop on privacy offered by the American Probation and Parole Association. We also visited the Privacy Coordinator of the Canadian Penitentiary Service.

The major files held in the Ministry of Correctional Services which we examined and which would be considered to contain sensitive personal information are described below.

a) Inmate files are held in individual institutions. An inmate's file moves with him/her from institution to institution and is maintained following final incarceration at the last institution. Copies of inmate files are also held in the Ministry's head office both in document form and on microfilm. The adult information system contains a computerized summary of the inmate's correctional record and reports are generated from this computer system on microfilm for use by head office staff for management and planning purposes.

b) Ontario Parole Board files are in document form and contain information on parolees and parole applicants.

c) A probation and parole computerized system contains summary information on inmates or parolees similar to the inmate adult information system. Probation files are kept in individual probation offices.

A. Policy on Confidential Information

The Ministry has an extensive written policy, contained in the Ministry's Manual of Administration, on confidentiality and the release of personal information. The policy details how written and telephone inquiries should be handled according to the inquirer -- whether police, courts, lawyers, news media, etc. It applies both to administrative offices

and institutions. For telephone requests, if the recipient of the call judges the request to be legitimate, only basic information may be given out; for example, the fact that the inmate is in the institution, the stated charge, the date of remand, the amount of bail or fine. No information about the inmate's release is given. Further information may be given to police, lawyers or relatives by a supervisor after first calling back to check the legitimacy of the call. Staff at the Ministry's central records section seem to be well aware of the policy and reasons behind it.

B. Inmate Records

Inmate files contain a number of standard forms. First, the inmate's record card contains the inmate's personal history, physical description, and information on charges, sentences, previous convictions and discharges. The card is initially filled out by institution staff when an inmate first arrives there, using information on the warrant of committal and also that obtained from the individual. In the case of someone serving a very short sentence of less than 30 days, or who is held on remand, this may be the only information the Ministry collects. A copy of the card is sent to head office where the Provincial Bailiff uses the information to decide on placement for the individual if incarceration is long-term (more than 90 days). The information is also entered for creation of the central computer file. Information

thereafter is updated through a daily log system and changes made to the inmate record card. The card provides a section for recording "traits" of the inmate in six categories: assaultive, disturber, sexual deviant, arsonist, escapee and suicidal. The sensitive nature of this information is indicated by the instruction that the appropriate box be checked in pencil only, and that the source and detail of the information should also be recorded. Before an inmate is transferred to another institution, the authority of the superintendent must be obtained for any "trait" assessments to be retained on the record.

All institutions each day submit to head office a log of significant events concerning inmates in their charge. Events such as transfers, temporary absences, misconducts, etc., are also keypunched to provide computerized management information.

An inmate's file also contains copies of standard forms recording transfers of the inmate between institutions, temporary absence permit applications, records of misconduct, etc. In addition, in many cases copies of both pre-sentence reports and monthly progress reports on long-term inmates completed by the institution staff are held in the file. It is probable that an inmate may already have seen a copy of the pre-sentence report or could get a copy from his/her lawyer. This would have been prepared by a probation officer and may contain comments about the individual's family or associates, or information gathered from them. However, although progress is discussed with an inmate, it is not likely

that s/he will have been shown a copy of the progress report which may contain observations about behaviour and attitude. We were shown inmate files selected at random containing observations which we doubt the authors would wish the inmates to see.

Within the institution we visited, inmate files were held in a central area adjacent to the superintendent's office. Files are only removed from the area if the prisoner is transferred to another institution or under a subpoena. Items of information on the file are made available on site to institution staff, police, National Parole Service, Legal Aid and the inmate's lawyer. All psychological and medical information on inmates is held at the inmate's institution in separate files to which access is strictly limited. Medical information is regarded as somewhat less confidential than psychological information because it may concern treatment the inmate needs (for example, insulin shots for diabetes) and it is vital to the inmate's health that this treatment be available wherever s/he goes. Both medical and psychological files are transferred with the inmate on movement to another institution.

The inmate file also contains information on the calculation of earned remission. The term "earned remission" refers to the amount of time, up to 15 days for every month served in prison, by which a term of incarceration may be reduced on the basis of good behaviour.⁴ At one

4 Ministry of Correctional Services Act, S.O. 1978, c. 37, sup., s. 28.

time, remission of sentence was automatic; now "slips" reporting unsatisfactory behaviour may be made to an individual's file. On that basis, the full term may have to be served. The inmate is given a copy of the slip if it is issued, and is made aware of the conditions under which remission may be earned. At the end of each month, an internal committee within the institution meets to consider all inmates and to decide if each individual has earned the monthly remission. There is an appeal process for the individual who is fully informed of this decision. Earned remission applies to all inmates sentenced for three days or more.

When an individual enters an institution, the Ministry's central records area attempts to match the individual to a previous file through a key card index, which has now been computerized. The institution takes fingerprints of inmates convicted of indictable offences and obtains, in those cases, a copy of the criminal conviction summary from the RCMP which is then maintained on the inmate's file. The criminal conviction summary or criminal record as it is more commonly known, is on a standard RCMP form with the fingerprint system (FPS) number from the conviction summary. A check on the computerized inmate file is made to determine whether the individual has been incarcerated previously in an Ontario institution. If there is no FPS number (in other words, those individuals not previously convicted of an indictable offence), a check is made against the computer file using the name, sex, date and place of birth to determine whether the inmate has previously been in an

Ontario institution. If this is the case, the fact is revealed, and the location of the last incarceration is indicated and hence the location of an inmate's file.

The Ministry of Correctional Services maintains a system of unique identifiers throughout its institutions. There is a unique main file number for each individual. The inmate is assigned another number for the purpose of each institution's filing system, every time s/he enters a new institution. This allows each transaction in the system to be recorded. Files on inmates are retained for 15 years following the last incarceration, and are then destroyed.

C. Probation Records

In Metropolitan Toronto, probation orders are administered at 12 offices, which handle approximately 8,000 probations at any one time. The Old City Hall office illustrates the typical function of the court liaison, and has some additional responsibilities. All probation orders from the provincial courts at Old City Hall and the nearby County Court are sent to this office. Probationers are interviewed to obtain basic personal information, permitting the officer to assign him/her to report to a probation office at a convenient time and location. All court liaison offices in this way perform the task of assigning the subjects of probation orders made in adjacent courts to appropriate reporting offices.

The Old City Hall office routes probationers to conveniently located reporting offices when persons come to Toronto from other centres while under mandatory supervision orders.

The terms of court orders may vary widely and are stated on the probation order form. In addition, the judge may specify his/her own terms. Once at the appropriate office, the client is assigned to a probation officer, who then provides supervision according to the needs of the client. In most cases this involves meeting with the client once a month to ensure that the terms of the probation order are met, but the officer may also help the individual to find accommodation and a job, and generally assist him/her in meeting the terms of the probation order. The Toronto office uses the Toronto Youth Employment Centre to help probationers get training and to find a job. Older probationers are often alcoholics or have drinking problems and are simply going through a revolving door. Others may be involved with fraud or white collar crime.

The probation office's working relations with the police have improved since the Metropolitan Toronto force set up the Bail Probation Order Unit. A list of all persons arrested in Metro Toronto is sent to the probation office once during each 24-hour period. A copy of the arrest list plus a copy of the court docket for the day is sent to each court liaison office. There, the probation officers may check whether any of their probationers have been arrested, and may learn the outcome of any

proceedings in which their charges may have been involved. The probation officer visits the probationer who has been arrested in breach of the probation order. In the case of arrested parolees who are supervised from the same offices, the parole board is notified. The officer may report the arrest of a probationer to the Crown attorney, who may then recommend that charges be laid or that the suspended sentence allowing the probation order be replaced by other terms. The probation officer then visits the person involved, and in the case of a parolee, notifies the parole board which considers whether to revoke parole. If it is felt that probation is not working, the probation officer may report to the Crown attorney who may recommend that probation be terminated, in which case the individual would have to return to court on the original charge.

Included in a probationer's or parolee's file is a copy of the probation order, and a copy of the pre-sentence report if one was ordered by a judge, or a copy of the parole notice. Either of these documents might have been the cause for initially opening the file. A "record of supervision" form is also completed, which includes a diagnosis of the individual's problems, the planned program for the probation period and a final summary on completion of probation. Any subsequent court appearances are also included on the record of supervision. Also, field notes from the probation officer's field book are kept in a closed file. These notes may be required to be produced in court in the case of a subsequent charge. Where information is to be gathered about

the probationer from schools, employers or other organizations, the probationer is asked to sign a "release of information" form, which authorizes the organization to release information about that person. There have been no reported instances of probationers refusing to sign a release.

In addition to supervision, probation officers are responsible for preparing pre-sentence reports where required to do so by a court order under section 662 of the Criminal Code, and this forms a significant portion of their workload. The offender must see the pre-sentence report, so a copy is usually given to defence counsel. Pre-sentence reports must be factual and cannot include recommendations, although this may become possible in the near future. The pre-sentence reports are seldom read out in court. Offenders have been known to leave copies of pre-sentence reports lying around or to give them to their families, which in some cases may cause problems because of comments about family history and background that may be included in the report.

Around 35% of probation files contain psychiatric reports. Psychiatric reports may be included on file when ordered by a judge, and reports are usually addressed to the probation officer. They are treated as confidential information, although they are included on the probationer's file for the use of the Probation Service. A summary of the psychiatric report only is given to other professionals in corrections, such as classification officers or community resource staff,

unless the psychiatrist's permission to release the report is obtained. The probationer's file is transferred from office to office within the Ontario system if the probationer moves location. Probation files are kept for five years and then burned if they are inactive, except for files on people with names beginning with "C," which are sent to Archives, presumably for research purposes. The central index is used to trace files if someone re-enters the system, in which case the file is reactivated. Reports by probation officers and pre-sentence reports have apparently improved in quality and objectivity as a result of better staff training. In the files we examined, the reports by probation officers seem to be more factual and more objective than the psychiatric reports. A 1976 study of the parole process by the Law Reform Commission⁵ commented on the need for clarity, consistency and uniformity in reports about inmates and parolees. It is obvious to us that continual attention must be paid to the objectivity of reporting.

Because their work is at the community level, probation officers work closely with other community organizations such as the police, the John Howard Society, schools, etc. There is a necessary informal sharing of information so that the officer may provide reports which are useful in court and in reaching parole decisions, and may also assess the progress of those in his/her charge. The possibility that probationers and inmates may be given access to their files is of considerable concern

5 Administrative Law Series, The Parole Process (Ottawa: Law Reform Commission of Canada, 1976).

to probation workers because of the often subjective nature of their reports and the fact that the sources of the information they collect may be noted in the documentation. They fear, as do workers of private agencies, that they could be subjected to a civil suit if such information is released and is proved to have been damaging in some way to the individual concerned.

However, it must be noted that the greatest potential for excessive invasion of privacy in the correctional field arises where a searching exploration of an inmate's private life outside the institution is made. Pre-sentence reports, for example, often contain personal information about the inmate's family, whose privacy must be considered as important as the inmate's. The rehabilitative model in corrections, as in other social services, may lead to the collection of personal information justified on the grounds of providing help. A balance must, however, be struck between the need for the information and individual privacy.

The computerized Adult Information System was started on April 1, 1975, and only information from that date has been included on the computer record. There has been no purging of the record to date. The system therefore contains all the information contained on the inmate record card for all people who have entered a correctional institution or jail since that time. The output from the system is on microfilm, and is intended for the use of operations management, the parole board, the

Provincial Bailiff and regional administrators. It replaced the laborious manual updating of duplicate files in several areas. Preparation of data for the system is carried out on the fourth floor of the Ministry's head office building, where all central files are also kept. The Ministry uses the Leaside Data Centre to process the data and produce the microfilm output. Old records which fell within the 15-year retention period have also been microfilmed and printed for distribution. The Ministry is proposing to implement on a trial basis a mini-computer system to provide operational data on inmates within the Toronto jail. There is currently no computerization of inmate records within individual institutions.

D. Ontario Board of Parole

The Ontario Board of Parole is responsible for considering parole for inmates in provincial institutions. An inmate serving a sentence of less than six months may apply for parole; all others are automatically considered.

Files on parolees are kept on the fourth floor of the Ministry of Correctional Services head office, in the central records area. An inmate's file contains a form recording the decision of the parole board which includes the individual's name, sentence information, names and addresses of spouse and parents, and the location and date of the

parole board meeting to consider the application. There is also a space on the form on which the decision of the board is noted following a meeting with the inmate. Parole board members use this space to record their impressions of the individual which are thus recorded in the inmate's file. Also included in a parolee's file are notices of release on parole, notices of parole violations and information as to the suitability of the person to be paroled. This latter form is filled out by a relative of the applicant or some other person designated by the parolee and contains information about the inmate's home, school record, types of companions, general reputation in the community, etc. It may also include comments about the candidate's home and could contain information about the individual's parents, wife or husband and the relationships between them. The information is used to assess the environment to which the candidate would return on parole. Parole files on individuals may also contain progress reports by probation officers.

In the estimation of parole board staff, approximately 20% of files contain confidential information which if released to the individual concerned, could result in a danger of some sort to the person who provided it. It was further estimated that about 40% of files would contain information which if the individual were to learn of it would cause strife within the inmate's family. An example would be where an inmate's wife had requested the parole board not to release the inmate because of family circumstances.

All psychiatric information on inmates maintained by the parole board is kept in a locked file within the Chairman's office and information is available only to board members who sign for it. The Ombudsman has on occasion been permitted access to individual psychiatric reports provided that release has been given by the person concerned.

E. Privacy Issues in Corrections

It is apparent that the Ministry of Correctional Services regards the confidentiality of information it retains about the people with whom it deals as a serious matter. Files on inmates are closely guarded. In the Ministry's head office, all personal records, including records about Ministry employees, are maintained on the top floor which is accessible only by elevator. In the institution we visited, files were kept in one central location to which access was restricted. In addition, the Ministry has an extensive policy on confidentiality and the new Ministry of Correctional Services Act⁶ has a section on confidentiality which reads as follows:

Every person employed in the administration of this Act including any person making an inspection, investigation or inquiry under this Act, shall preserve secrecy in respect of all matters that come to his knowledge in the course of his duties, employment, inspection, investigation or inquiry and shall not communicate any such matters to any other person except

6 S.O. 1978, c. 37, s. 10, sup.

- a) as may be required in connection with the administration of this Act, the Parole Act (Canada), the Penitentiary Act (Canada), the Prisons and Reformatory Act (Canada) or the Criminal Code (Canada) or the regulations thereunder;
- b) to the Ombudsman of Ontario or Correctional Investigator of Canada;
- c) in statistical form if the person's name or identity is not revealed therein;
- d) with the approval of the Minister.

No penalties however, are attached to contravention of this section.

While the sharing of information from an inmate's file with organizations outside of corrections is closely guarded, questions of data protection concerning personal records within the correctional system still need to be addressed. On the basis of information collected about an inmate, decisions are made as to the kind of institution to which s/he is to be assigned, any special treatment s/he is to receive, whether s/he will or will not be granted a temporary absence permit, etc. Although an inmate may be aware of much of the information leading to these decisions, s/he is not normally permitted to see the actual file. An inmate is, of course, likely to have already seen the pre-sentence report, the warrant of committal and receives or is shown copies of misconduct reports, temporary absence applications, etc. An inmate may not, however, see the inmate record card (which may indicate that s/he is assaultive, a sexual deviant, disturber, or an arsonist) nor may an inmate generally know the contents of the progress reports or psychiatric assessments. As was pointed out by some of the correctional staff with whom we spoke, a notation on a file may cease to be applicable but may remain on the

file unless it is specifically removed by a member of staff who decides it is incorrect. In addition, when files from previous sentences are referred to, out of date information could influence a decision about an inmate. Although such occurrences are likely to be rare, there is a need to protect against erroneous data. The person with the keenest interest in ensuring accuracy of information is the inmate. It was, however, also pointed out to us that corrections is very much an adversary system and that what may be a rational suggestion to govern data protection in other areas of record-keeping, may result in unexpected distortions in the correctional field. We note that the volume of applications to view files received by the Canadian Penitentiary Service, largely from inmates currently serving sentences in federal institutions, was in excess of 5,000 after only three months of operation of the Canadian Human Rights Act. Over 90% of federal inmates will have passed through provincial institutions, and under a provincial access scheme it could be expected that many of them will ask for access to their provincial records. This is in addition to the demand from provincial inmates which is difficult to estimate, except to note that almost 13,000 inmates were in the custody of Ontario institutions during 1977 compared with about 10,000 in federal institutions to give an indication of the relative populations.

The problems of providing individual access to files in the correctional field are therefore similar to those affecting policing: protection of third parties and the possible volume of requests. In addition, there

is the possibility that an inmate's correctional program may be adversely affected by revealing the full file to him/her, particularly where psychiatric information is concerned.

The Canadian Human Rights Act⁷ grants rights of individual access to personal records. It also provides specific exemptions which may be applied to access to inmate records:

The appropriate minister in relation to a government institution that has control of a federal information bank may provide that subsection 52(1) or any provision thereof specified by him does not apply in respect of a record or part thereof concerning an individual in the information bank where in the opinion of the Minister knowledge of the existence of the record or of the information contained therein

- a) might in respect of any individual under sentence for an offence against any Act of Parliament
 - i) lead to a serious disruption of that individual's institutional parole or mandatory supervision program,
 - ii) reveal information originally obtained on a promise of confidentiality express or implied or
 - iii) result in physical or other harm to that individual or any other person.

8

A serious inconsistency in the wording of exemptions (ii) and (iii) is that they only apply to individuals under sentence. We believe that if the exemptions are valid while an inmate is in an institution, they remain valid when the inmate is released. With this modification, the exemptions would seem to grant the maximum protection from any danger

7 S.C. 1976-77, c. 60.

8 Ibid., s. 54.

inherent in the release of an individual's file. In addition, the Act permits regulations to be made precluding the release of medical records, including psychological reports, to an individual where it would not be in the best interests of that individual.

The final question is therefore one involving the workload required to handle applications and review files in order to apply exemptions. Some alternatives for implementation suggest themselves:

1) Automatic access could be granted in the case of non-evaluative reports, such as the inmate record card, misconduct reports, etc., and to documents which would have been revealed in court (e.g., the pre-sentence report). These records presumably form the official file on the individual and contain a history of information and decisions about him/her. In order to phase-in the right of access for the first year, access could be provided only to new files (created after implementation of the Data Protection Act). Following the first year, retroactive access could be granted in stages. This would permit the Ministry to organize new files on inmates in such a way as to facilitate access to them. It would also enable experience to be gained in living with an access scheme. It is likely that exemptions to such records would need to be applied only on rare occasions.

2) Evaluative reports, such as progress reports and information which would reveal confidential sources, could be kept separately from non-

evaluative reports. Again a phased-in right of access could be adopted. In addition, if it was considered that the costs of applying exemptions to old files would be prohibitive, the right of access could be granted only to files started after a Data Protection Act was implemented. Undoubtedly this would result in some changes to the way in which reports are written, and might result in greater objectivity; however, there might also be some loss of useful but subjective data, although it is impossible to assess the extent to which this might occur.

F. New Developments

The institutional inmate files are presently being computerized, and will be linked to the centrally-stored Adult Information System. In this way, the record of identifying data and information concerning the location of the inmate, his/her court dates or sentence disposition, and an entry indicating whether a medical examination has been performed is automated. Within a few years it is anticipated that the institutions within the Metropolitan Toronto area will all be using this type of facility.

With this linkage to the central Adult Information System which contains historical material concerning the inmate's past incarcerations, it will be possible to transmit data from an institution to the central data bank. In this way decisions concerning the best institution and

treatment for an inmate may be made rapidly and with the most up-to-date information available at the central location.

CHAPTER XIV

PERSONAL PROPERTY SECURITY REGISTRATION

The computerized Personal Property Security Registration system, administered by the Ministry of Consumer and Commercial Relations, was created in April, 1976. In effect, the system amalgamated and automated a number of separate manual files used in the registering of personal property as security against loans. Prior to the introduction of the computerized system, each county and district used separate manual systems for registering security agreements. A person requiring information could search through an index book and request the original security agreements from the files.

The Personal Property Security Act¹ applies to every transaction that in substance creates a security interest, including a chattel mortgage, conditional sale, equipment trust, floating charge, pledge, trust deed or trust receipt, and an assignment, lease, or consignment intended as security. Security for both individual debtors and business debtors are included on the file. The credit grantor provides a completed registration form from which all information is taken and recorded on the computer file. Information regarding the registration presumably comes from documents concerning the original security; however, no record

1 R.S.O. 1970, c. 344.

is kept of these original sources, nor are they identified on the record. The minimum amount of information required to register a security is the name and address of the debtor, the secured party (i.e., the creditor) and the collateral classification. The principal amount secured is required to be stated only with respect to security provided by individuals in a consumer transaction. No principal amount secured is required to be stated for security provided by businesses. According to the system's Registrar, the reason for this difference in treatment is that individuals are in greater need of protection against over-burdening themselves with credit, whereas businesses are generally examined more searchingly before loans are made to them. There is no requirement that the debtor be notified of the security's registration in the PPSR system. Consequently, there is no requirement that the debtor attest to the accuracy of the financial information provided.

Under the old manual system, information was much more open to access because anyone could examine the entire index book held by a county or district, as well as the original source documents. Early in the development of the PPSR system, some consideration was given to assigning the task of organizing an integrated registration system to private industry. However, in order to protect the public, it was decided that this function should continue to be performed by government. The amount of information required for the new system was reduced to the minimum because of questions relating to data confidentiality and privacy.

With the PPSR system, both computer and manual checks are made to ensure the accuracy of data entered into the system. All input documents (registration forms) are microfilmed for backup control and audit, and original source documents are, of course, retained by the parties. Access to the data entry area is restricted to authorized persons only. Processing is carried out at the Downsview Computer Centre. All registration forms are stored in the Records Centre at Mississauga.

Once the debtor has paid his obligation in full, the secured debt is discharged. The Act does not require, however, that the creditor update the register by filing a notice of the discharge. Section 54(1) and (3) of The Personal Property Security Act does provide that the debtor may demand that the secured party provide him/her with a discharge of the registration after the debt has been paid. If the secured party fails to provide it, s/he is subject to a fine of \$100 plus any damages resulting from the failure. To the Registrar's knowledge, this fine has never been imposed.

Two searches may be made of the individual debtor file. First, the file may be subjected to a specific search, for which given name, surname, initial of the second given name, and date of birth are required. Since as a general rule, the property constituting the collateral cannot be identified uniquely, data about the debtor is the only way to identify information on the file. In the vast majority of cases, the information required for a specific search will reveal only one record.

Second, the most common type of search, the non-specific search, requires only the first given name and the surname. Usually, an individual seeking to search the file will not have the date of birth and initials, and must first request a non-specific search, which may reveal a list of names of people from across Ontario. The Registrar has indicated that with respect to privacy, this is an improvement over the old manual system, where the total list of names on file in any particular county was open to anyone who requested access. Under the PPSR system, a more limited list of people of the same name is provided to a requestor. When the PPSR system was being developed, a number of possible identifiers were examined, including the social insurance number; however, all of these were discarded in favour of names and dates of birth, although it was recognized that often the date of birth is neither accurate nor easily obtainable.

A registration on file will exist for three years, unless the registration is discharged by the creditor (and this is done by only a small percentage of creditors). Thus, information on file is likely to become out-of-date if the loan is paid off. The Registrar pointed out that 30 months is a popular financing period, and is close to the current three-year retention span on the PPSR system. However, due to increasingly lengthy financing terms, there has been pressure to extend the retention period to five years. Currently, though, when the three-year retention period has expired, the registration is automatically removed from the system, without the secured party being informed. It is possible, however, for the creditor to register a "renewal statement,"

extending the effect of registration for a further three years.

The Personal Property Security Registration system is operated on a cost recovery basis. A schedule of fees for registration and inquiries has been established. In addition, daily tapes are sent to the Associated Credit Bureaus of Canada which distribute information from the tapes to their members. This service is carried out on a contract basis for a fee which recovers the cost of tape processing and transmission. Additionally, the Ministry contracts with Dun and Bradstreet to provide daily information from the system on business debtors and securities.

Four main issues have been raised regarding privacy and the PPSR system. First, information in the PPSR file is sold to credit reporting associations, a purpose for which privacy advocates claim the system was not originally designed. Second, the principal amount secured, which is information required for consumer goods, is often included on the file with respect to other classifications of collateral. Third, a non-specific search of the system, although less privacy invasive than the old manual system, may reveal a list of people with the same name. The fourth issue concerns the discharge of a registration by the secured party, and the fact that the system may contain information which is neither current nor accurate.

The first three criticisms of the system hinge on the interpretation of the purpose of the Personal Property Security Registration system, and

on the balance between individual and public interests when considering whether disclosure of information on file represents an unwarranted invasion of privacy. The Personal Property Security Act provides a means of registering a document (the financing statement) so that a security interest may be "perfected" under the terms of the Act. A security interest can also be perfected with respect to some kinds of collateral by other methods, e.g. by possession. Section 44 of the Act states that:

- (1) Upon the request of any person and upon payment of the prescribed fee,
 - (a) the registrar shall issue a certificate stating whether there is registered at the time mentioned in the certificate a security agreement or other document in which the person named in the certificate is shown as a debtor and, if there is, the registration number of it, and any other information recorded in the central office of the registration system;
 - (b) any registered security agreement or other document shall be provided for inspection at the branch office where it was registered; and
 - (c) a certified copy of any security agreement or other document shall be furnished at the branch office where it was registered.

This provision means that the Registrar is permitted to provide information about anyone named in the PPSR file to anyone who requests it. Presumably, one of the purposes of section 44 is to enable a free flow of information among people who are involved in transacting financial business. Because credit reporting associations are key institutions in the business community, to the benefit of both lenders and borrowers alike, we do not believe that providing them with financial data about people with whom they may deal is unduly

invasive of privacy or is inconsistent with the Act. The Consumer Reporting Act² regulates the kinds of information which credit reporting agencies may collect, and the uses to which it may be put. However, privacy interests would be better protected if debtors were made aware of the public accessibility of the PPSR system when their names are first registered on the file.

The use of information on the file for purposes other than to establish credit worthiness or to protect a security is another problem, one which is presented by all large publicly accessible files. It is possible, for example, to obtain a listing of all John Smiths in Ontario who are on the file, together with their addresses, dates of birth and financial liabilities. We are uncertain whether this is qualitatively different from obtaining information about any particular John Smith or groups of John Smiths in the file. The records are purged every three years, so that an address history beyond that time period cannot be established. The file might be further protected from uses beyond its original intent by requiring more identifying information about borrowers, such as address, telephone number and place of birth. However, this information would be much more invasive of borrower privacy than that presently collected. Taking all interests into account, we can only conclude that the present loss of privacy made possible by a general search of the PPSR system is simply one of the costs associated with a large, publicly accessible and publicly useful file.

2 S.O. 1973, c. 97.

The fourth issue concerning the currency and accuracy of information within the file poses a more serious problem. Although debtors have the right under The Personal Property Security Act to demand that a discharge be provided after the debt has been paid, and penalties exist for non-compliance with such a request, it seems unlikely that consumer debtors would be aware of their rights in this regard and would take steps to register a discharge. Without a statutory requirement that creditors send in notices to the PPSR system, no real incentive exists for the creditor to report changes in file status.

Finally, we raise an additional issue which we believe is more important than any of those previously mentioned. People are not informed that their names will be placed on such a totally accessible computer file. It seems that this is the primary issue from which the others flow. If people are unaware that such a record exists, they cannot know of the right to correct it when the debt is paid, nor that such information will be available to anyone who requests it.

As a means of notifying people that a record of the financing arrangement will be placed on the PPSR system, we suggest that consideration be given to the inclusion in The Consumer Protection Act³ of a requirement that lenders provide such notice to borrowers. In addition to a description of the system, the notice could include information with respect to those statutory rights concerning discharge.

3 R.S.O. 1970, c. 82.

CHAPTER XV

LICENSED DRIVER AND VEHICLE OWNERSHIP RECORDS¹

The Ministry of Transportation and Communications is responsible for administering The Highway Traffic Act. Under this Act, all drivers in Ontario are required to complete successfully an examination of their driving skills and to be duly licensed, and all vehicles operated on public highways are required to be registered.² The only exceptions to the requirements concern out-of-province drivers and vehicles, which need not be licensed or registered until in the province for specified periods of time. Under the authority of section 145 of the Act, the ministry maintains records of all drivers and vehicles in Ontario in two separate computerized files. These records are used by the Registrar of Motor Vehicles, by police officers and by the courts to enforce the Act. As we shall see, portions of these files are also used by insurance companies and employers and are open to the general public upon payment of a flat fee.

1 Other studies of driver and vehicle record systems and their implications for individual privacy have been performed by James B. Rule, "Vehicle and Driver Licensing in Britain," in Private Lives and Public Surveillance (New York: Schocken, 1974); and Daniel H. Lufkin, "The National Driver Register," in Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education and Welfare (Boston: Massachusetts Institute of Technology, 1973).

2 The Highway Traffic Act, R.S.O. 1970, c. 202, Part II, s. 6 and Part III, s. 13.

A. The Licensed Driver File

The licensed driver file is fully computerized and contains information on more than five million Ontario drivers. Basic information on the file is provided by the individual through the application form for a driver licence. The information contains the name, address, height, age, date of birth³ and the individual's Ontario driver licence number. The driver licence number contains coded information on surname, given name and middle initial, the sex of the individual and coded information on the month, day and year of birth. This creates a unique driver licence number for each individual on the file.

An applicant for an Ontario driver licence must complete the form designated for the particular class of vehicle s/he wishes to drive, among eight classes of vehicles described in the Act. Three "Medical Grade Codes" delineate which one of the three form types pertains to each class of vehicle. These codes refer to medical condition, visual acuity and age requirements for licensees. The most searching examination is made for school bus driver applicants, who must undergo a medical check, as well as a criminal record check made by the OPP Criminal Records Branch to determine whether the individual has been convicted of a morals charge or for drug trafficking or drug use.⁴

3 According to Ministry officials, applicants must verify their identities by presenting birth certificates, landed immigrant papers or other documentation.

4 According to Ministry officials, a criminal record check for driving instructors will also be included in the regulations in the near future.

TABLE XV.1

ONTARIO CLASSIFIED DRIVER LICENSING SYSTEM
QUICK CHECK CHART*

[illegible]

DECEMBER 1, 1976

* Source: Ontario Ministry of Transportation and Communications

At present a question on the application form for a school bus driver licence asks whether the individual has ever been convicted of a non-motor vehicle offence under the Criminal Code of Canada or The Narcotic Control Act. The computer file does not contain any information from the criminal record (except for information about traffic offences), but merely an indication that the record check has been done in accordance with the requirements of the Act.

Similarly, where medical suitability of the individual is required, i.e., for persons who are licensed to operate trucks and buses, the computer record merely notes that the medical report has been received.⁵ The contents of the report itself are filed in document form. Drivers of buses, school purpose buses and tractor-trailers are required to provide satisfactory medical reports every third year. Once such drivers reach the age of 65, they are required to provide medical reports annually to retain these higher classes of licences. Until the age of 80, applicants for "Class G" licences to drive most automobiles and small trucks are not required to be medically tested. The only medical information required to obtain Class G licences indicates whether the applicant is subject to epilepsy, convulsive disorders, dizzy spells or any condition that causes unconsciousness. In such

5 To determine medical suitability, the Registrar gives the applying individual a medical form to be completed by the physician of his/her choice. The form also contains an authorization for release of hospital-held medical information about the applicant. Upon receipt of the completed form, the Registrar makes the decision as to the applicant's suitability. To assist him in this function, the Registrar may call upon the Medical Advisory Board.

cases the individual may be required to obtain a fuller medical report from one or more licensed physicians. The resulting computer file simply indicates that a medical condition exists, but the medical report itself is filed in document form. At the age of 80, yearly medical testing becomes mandatory, although the Ministry may require anyone between 70 and 80 to pass a medical test if his/her driving record deteriorates. Medical reports are kept in the manual file for the life of the driver.

Under the Act,⁶ all medical reports are protected from disclosure. The Registrar has interpreted this section to mean that even record subjects may not have access to medical information about themselves. The rationale given for denial of subject access is that the medical report is supplied to the Ministry on a confidential basis. It is therefore believed that the responsibility for providing or refusing subject access lies with the doctor who provided the medical information to the Registrar.

Under section 143 of the statute, medical practitioners must report to the Registrar the name, address and clinical condition of every person 16 years of age and over who is suffering from a physical or mental condition (including habitual drunkenness and narcotic addiction) that may make it dangerous for such a person to operate a motor vehicle.

6 The Highway Traffic Act, R.S.O. 1970, c. 202, s. 143(3).

Section 144 requires every optometrist to similarly report the identity of every person 16 years of age or over who is suffering from an eye condition that may make it dangerous for that person to operate a motor vehicle. The law specifies that such reports from doctors and optometrists are privileged for the information of the Registrar only and are not open to public inspection. In addition, such reports are inadmissible in evidence for any purpose at any trial except to prove compliance with the reporting requirement. Precise and easy-to-measure standards of vision have encouraged a high level of reporting from optometrists. Because assessments of general medical conditions are based largely upon opinion and judgment, which may be called into question, medical practitioner reporting has not reached the level of optometrist reporting.

Vision and other medical data received by the Ministry⁷ are regularly reviewed by an internal Medical Advisory Board, which recommends to the Registrar whether or not to suspend a driver or to require further examinations or documentation from other doctors. In making recommendations regarding the seriousness of conditions warranting suspension, the Board utilizes standards formulated by the Canadian and Ontario Medical Associations. Whatever the Board's recommendations, the final responsibility for licensing decisions rests with the Registrar. The Registrar notifies by mail all those whose licences have been suspended

7 Such information may also originate from non-medical sources, such as concerned family members.

or revoked for medical reasons. The notification contains the "general basis" upon which the Registrar's decision was made. An individual whose licence is suspended in this fashion may appeal to the Licence Suspension Appeal Board and further, to a Judge of County Court. To present his/her appeal, a suspended driver may wish to use information in the medical report held by the Ministry. However, present Ministry policy does not permit the appellant to actually view the report. Instead, according to Ministry officials, the "essential facts within the report" are told to the appellant upon his/her request. In cases where the Registrar believes certain information within the report, such as a diagnosis of cancer, may be harmful to the requesting individual, that information will not be revealed.

The Licenced Driver file also contains information on convictions of driving offences, by demerit points resulting from such convictions, and suspensions and reinstatements of an individual's driver licence. Demerit points are retained on the file for a total of five years. The computerized information is suppressed after the third year so that it will not be revealed by a general inquiry to the file. Criminal Code driving offences and other information recorded on the file are purged according to a detailed administrative manual schedule, but certain data items, such as the date of first licensing, are retained permanently.

Regarding access and use of driver licence file information, three years of driver history information can be obtained by anyone from the file upon written request and payment of a \$3.00 fee which, the Ministry maintains, deters the "merely curious." Regarding release of information from the driver file over the telephone, unwritten policy dictates that information be given to police, courts, lawyers, employers, insurance companies and the record subject, provided that adequate identification is given. Identification requested may include name, address and driver licence number, all of which are readily verifiable by computer terminal. The police and Crown attorneys may obtain a complete 5-year driver record in typed form, including convictions, driver status and information about suspensions and demerit points. In 1976, there were 160,000 requests for driver history abstracts from the police. Researchers may also be given information from the file for projects attempting to improve driver safety or driver education.

Other inquirers are given only basic information which they specifically request, such as licence expiry date, demerit points and suspensions -- the most common items of interest. In 1976, there were one million requests for driver history abstracts from the general public. Certain information on the file is not accessible to the general public; specifically the driver's previous address history, which is available only to government, law enforcement agencies, lawyers, and insurance companies concerned with matters involving a motor vehicle. In 1975, there were 7,781 searches of driver address history for lawyers and 211

for insurance companies. The Ministry specifically suppresses driver address history to prevent requests from finance companies and collection agencies wishing to trace individuals. However, it should be noted that because requestor identity is difficult to verify completely by telephone, some personally sensitive information may inadvertently be revealed to these parties.

No logging mechanism has been installed in the system to track the origin or identity of specific inquiries. Therefore, no record subject could obtain a list of requestors, or the number of requestors, accessing his/her driver record during a given period of time. In contrast, the United States National Driver Register was designed in such a way that information transfer lists could readily be provided to record subjects.⁸

The Ministry policy that all driver records prescribed under section 145c of The Highway Traffic Act be deemed public information is consistent with policies of all other provinces, the territories of Canada and every state in the United States. The Ministry supports the use of these records by insurance companies and employers of drivers because experience and research show that the type as well as the number of convictions for violations of traffic laws are important in predicting future driving performance. The use of driver records for this purpose is consistent with the Ministry objective of improving highway safety.

8 Lufkin, Daniel H., op.cit., 219.

Many jurisdictions (e.g. Great Britain) give the police preferential access to certain data from driver registries. In Ontario, police access has been facilitated by a sophisticated computer communications system. Five-year driver histories (excluding medical information) may be accessed directly from the MTC computer by the Canadian Police Information Centre system (CPIC), which high-speed transfers the information on request to 250 law enforcement computer terminals in police stations and patrol cars throughout the province. To obtain print-outs from the terminals, police officers must identify queries by either driver licence number or driver's name, sex and date of birth. Following a query, the computer system delivers the driver history in a matter of seconds. Because of the information's availability at time of arrest, enforcement of suspensions has more than doubled since implementation of the CPIC-driver file connection.

B. Vehicle Registration System

Information on passenger vehicles and trailers is also computerized. Information about all other types of vehicles (trucks, snowmobiles, etc.) is on a manual system. The file contains information on the type of vehicle, the owner, and the company with which the vehicle is insured. Searches of the system may be made by the name of the owner, the registration number of the vehicle or by date. A listing may therefore be obtained of all vehicles currently owned by an individual

or by a company, or describing all vehicles owned by an individual or company in a given time period. Special computer programs may "call" the file by other characteristics, to identify, for example, all individuals owning a particular year and model of car.

For \$3.00 per vehicle inquiry, anyone who makes a written request may obtain information from the vehicle file. To receive information by telephone, the requestor's name and address must be previously listed with the Ministry and inquiry fees paid in advance. Hospitals, universities, apartment building and parking garage owners attempting to control illegal parking, collection agencies, and investigatory agencies are, according to Ministry officials, among those permitted to receive telephone information. The list is not maintained to protect record subject privacy but to ensure that the Ministry is duly paid for its services.

In the government sector, agencies making regular use of the file (without charge) and their specific purposes include: the Ministry of the Attorney General, to locate car owners with outstanding parking tickets; the Ministry of Consumer and Commercial Relations, to verify automobile lien registrations on the Personal Property Security Registration System, to investigate Accident Claims Fund claims and to produce information for Motor Vehicles Dealers Branch investigations; the Ontario Provincial Police, to identify car owners suspected of leaving the scene of an accident or other crime; and the RCMP, to identify suspects in certain crimes.

Police receive preferential access to motor vehicle information in two ways. In addition to its availability 24 hours-per-day, 7 days-a-week through a Ministry of Transport telephone connection for the exclusive use of the police, vehicle information may be accessed directly from the Ministry computer by the police through the CPIC system, in the same fashion that driver licence information is accessed.

Our research indicates that because the file is both readily available and easily manipulated, privacy invasions may occur. One case brought to our attention involved a woman claiming harassment by a law enforcement official who, after issuing the woman a summons, obtained her address from a check against the registration number of her car. Another involved a false arrest due to lack of updated information on the file.

The Ministry itself has received no complaints of false arrest, but has frequently handled complaints involving either parking tickets summonses or towing charges. In the case of parking ticket summonses, a six-week lag time between actual registration changes and the recording of those changes on the vehicle computer system occasionally results in the attribution of parking offenses to the former rather than the present car owner. The Ministry has instituted a special procedure whereby vehicle owners issued such mistaken summonses may quickly clear their names. The same lag time between actual registration changes and system updates may also prevent authorities from accurately identifying the owners of cars towed away for snow removal purposes. In these cases, the Ministry has paid any towing charges resulting from its mistakes.

Aside from computer updating problems, other difficulties which may arise from inaccurate ownership information on the file were pointed out to the research group. When a vehicle is sold, it is the responsibility of both vendor and purchaser to transfer the ownership. If the vendor signs the ownership change, but the purchaser does not notify the Ministry of such change, the vendor will receive any parking tickets accumulated by the purchaser, because the only information on the file available to the police is the original owner's address. In addition, a judgment could be launched against the original owner because the ownership has not changed. Staff of the Ministry indicated that the general public does not seem to be fully aware of these implications. The sensible practice is for an owner to keep the vehicle until the ownership change has been made, or to personally transfer the ownership.

Bulk information from the vehicle file was at one time sold for one cent per record to the R.L. Polk Company which developed mailing lists for sale to business companies. However, in 1974, this practice ceased because of public concern about use of government records for commercial purposes. The primary information now sold to the Polk Company in bulk lists new vehicle registrations, which are subsequently sold to automobile manufacturing companies for the purpose of recalling vehicles with mechanical defects. Auto parts manufacturers or retailers may also buy address lists, which do not include owners' names, for specific marketing purposes. Agreement not to use information for sales

promotions or other purposes beyond that originally intended is specifically stated in contracts between the Ministry and commercial companies. However, the assurance of confidentiality is not otherwise protected in law.

C. Collision Reports

The Ministry also maintains a separate file consisting of collision reports, which are sent to the Registrar by police forces investigating accidents. Accidents involving personal injuries or damage to property apparently exceeding \$200 must be reported to the nearest provincial or municipal police officer, who is required to report to the Ministry within 10 days on the particulars of the accident, the persons involved, and the extent of the injuries and damage. The reports are retained on microfilm by the Ministry.

Information on traffic accidents is generally not made available over the telephone. Photocopies of the police report are provided to anyone upon payment of a \$5.00 fee. In 1979, 45,000 paid requests for photocopied reports were received by the Ministry. Collision report information is usually requested by lawyers representing persons charged with criminal offences or by accident victims bringing civil suits. Information from the collision reports file is also used by the Ministry to identify high-percentage accident locations for the purpose of correcting highway design and highway sign-posting.

D. Privacy Considerations

The existence of driver and vehicle records raises three privacy issues. The first concerns the creation of mailing lists from these files for use by private companies. Because the Ministry has ceased providing the Polk Company with information from the files for this purpose, the issue has been effectively dissolved. Companies could, of course, attempt to develop name and address lists by individual inquiries of the file, but the time and the cost involved would be clearly prohibitive. However, no restriction in statute or regulation prevents the Ministry from resuming the practice. In fact, since 1974 the Ministry has begun to sell address lists to automobile parts retailers for marketing purposes.

An increasing number of states in the United States restrict the use of motor vehicle registration information for commercial mailing purposes.¹⁰ The U.S. Privacy Act expressly prohibits a federal agency from marketing mailing lists for profit.¹¹ There is a conflict, however, between the Privacy Act and the Freedom of Information Act, which allows lists kept by numerous federal agencies to be copied on request. In Wine Hobby USA v. IRS, the Third Circuit Court of Appeals held that release of the

10 Alaska, Arkansas, California, Connecticut, Hawaii, Massachusetts, Missouri, Nevada, New Jersey, Ohio, Pennsylvania, South Dakota, Virginia, Washington and Wyoming, as cited in U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society (Washington, D.C.: USGPO, 1977) 127 and California Information Practices Act of 1977.

11 5 U.S.C. 552a(h).

registration list of persons making wine for personal consumption for direct-mail solicitation was not a disclosure required by the Freedom of Information Act because the purpose did not justify the potential invasion of personal privacy.¹²

The question of mailing lists was studied in some depth by the U.S. Privacy Protection Study Commission, which concluded that an outright ban on the provision of name and address lists compiled by government agencies to other public and private agencies would not be desirable, particularly because non-profit organizations would have difficulty in reaching their audiences without such lists. The Commission recommended, however, that government agencies be directed to devise procedures whereby individuals could express their wishes that any personal information held by the agency not be used for direct-mail marketing or solicitation purposes. The simplest method suggested by the Commission was the "negative check-off option," which would permit an individual to have a notation made on the file at the time information was collected, stating that s/he did not wish to receive unsolicited mail. Under the arrangement suggested by the Commission, any private-sector public record compiler "would still be able to copy the record, but it would be on notice that the individual had objected to use of his name, and presumably, for economic reasons, would not include that name on lists it develops for its clients." Any record compiler would also be

12 Wine Hobby USA, Inc. v. IRS, 502 F 2d 133 (3d Cir. 1974), as cited in U.S. Privacy Protection Study Commission, op.cit., 131.

obligated to inform other mailing list compilers of the record subject's wishes. In making these recommendations, the Commission relied on testimony which emphasized "the mailing list user's much stressed desire not to send messages to individuals who do not want to receive them."¹³

Rather than depend upon the good intentions of mailing list compilers, we recommend that the Ministry remove all names of individuals who exercise the "negative check-off option" from vehicle lists prior to their sale. According to Ministry officials, a programming procedure was devised in the early 1970's to remove the names of consumers complaining about "junk mail" from vehicle lists sold to the Polk Company. Re-instituting such a procedure should not be overly costly or time-consuming to the Ministry. We suggest further that individuals supplying personal information to any of the Ministry files be informed, at the time data is originally collected, of all intended uses of requested information. Record subject controls would be facilitated by accurate computer logging of outside information requests, particularly from commercial enterprises.

The second issue surrounding driver and vehicle files concerns their availability to the public. We accept the Ministry's view that the dissemination of information regarding driving history and vehicle ownership to employers of drivers and to insurance companies is consistent with efforts to improve highway safety. In addition, the public has a

13 U.S. Privacy Protection Study Commission, op.cit., 151-153.

need for ownership information in conducting transactions regarding vehicles. Privacy problems appear to arise only when this information is used for other purposes -- to trace debtors or to make judgments about employment suitability in positions where driving skills are not required. The Ministry has taken steps to minimize access to address history. It may be difficult to install other protections without adding significantly to the operating costs of the two systems. The sheer volume of inquiries (one million annually on the driver file alone) could prevent the introduction of an enforceable means of filtering out inappropriate requests for information.

However, we do recommend that the example of several other jurisdictions which regulate uses of driver files be followed. Specifically, we suggest that appropriate file uses and penalties for improper file use be established in law. Such protections might improve the current situation, in which any use of the information is effectively permitted.

We would also suggest that formal written policies be developed to restrict the provision of personal information over the telephone. Such policies might prevent abuses of the type previously noted.

The presence of driver and vehicle files raises a third privacy issue, the potential intrusiveness associated with police uses of file data for identification, investigation and surveillance purposes. At present, police are given extremely preferential access to both driver and vehicle

files in Ontario. Unlike any other agency or members of the public, the police may obtain complete driver and vehicle information directly from the MIC computer bank, through a system which combines driver and vehicle data with Canadian Police Information Centre system (CPIC) data and displays requested output on computer terminals located in police stations and patrol cars. Regarding vehicle files, the police may obtain not only the owner name and address for a specific vehicle registration number, but also, by making a special request to the Ministry, general name and address lists associated with any of several vehicle characteristics stored in the system.

Police use of the files to identify and trace individuals involved in specific vehicle-related crimes is accepted as a legitimate purpose by most jurisdictions. So too is police use of the files to identify those suspected of committing serious crimes, such as murder and armed robbery. Without access to such records, the police in highly mobile societies would be severely disadvantaged in their attempts to enforce the law.

However, direct police access for any purpose to what is, in effect, a registry of the names, addresses and certain personal characteristics of the large majority of Ontario's adult population, is more questionable from a privacy protection standpoint. If a proposal were introduced in this province to establish a general population registry of names and addresses for law enforcement purposes, it would doubtless meet opposition from many members of the public concerned about privacy. Yet, law

enforcement authorities have essentially obtained such a registry through the Ministry of Transportation and Communications computer systems. As testimony before the American PPSC revealed, law enforcement officials have sometimes exploited this privilege to increase their basic investigative capacities associated with a myriad of intelligence gathering and non-specific crime prevention activities. For example, the American Internal Revenue Service made plans to utilize a list of certain types of cars to facilitate a search for individuals who had not filed tax returns.¹⁴

In his study of British vehicle registration and driver licensing systems, Professor James Rule drew attention to their inherent "capacity for social surveillance," notwithstanding their relatively unsophisticated nature. In Dr. Rule's terms, the system's centralization of data, its sheer size and the speed of information flow and decision-making all make British driver and vehicle files amenable to social surveillance. The absence of detailed or particularly "sensitive" data on the files does not erase privacy concerns, as his research showed that "the most succinct and telegraphic data can often be the most potent in activating mechanisms of social control."¹⁵

Certainly, preferential police access to vehicle and driver licensing files has contributed to the government's capacity for social surveillance

14 U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society (Washington, D.C.: USGPO, 1977) 134.

15 Rule, James B., op.cit., 116-120.

in this province. Considering the broad scope of Ontario police activities, and the tendency of the police to obtain personal information from several non-enforcement related government programs (as detailed in Chapter XII), the following controls over police use of licensing and vehicle information may be desirable. First, all law enforcement uses of driver and vehicle information should be public knowledge in a regularly updated and commonly available document. Second, individuals who believe they have been subjected to privacy abuse or false arrest through information from the files should have the opportunity to pursue an easy avenue of complaint. Third, uses of the files for general "fishing expeditions" by law enforcement authorities should be closely watched and in some cases curtailed. We suggest that an independent data authority may be a good mechanism for instituting such controls and making decisions regarding appropriate law enforcement uses of driver and vehicle registration systems.

COMMISSION RESEARCH PUBLICATIONS

The following list of research publications prepared for the Commission may be obtained at the Ontario Government Bookstore in Toronto, or by mail through the Publications Centre, 880 Bay Street, 5th Floor, Toronto, Ontario M7A 1N8.

Prices are indicated below. Orders placed through the Publications Centre should be accompanied by a cheque or money order made payable to the "Treasurer of Ontario."

Further titles will be listed in the Ontario Government Publications Monthly Checklist and in future Commission newsletters.

The Freedom of Information Issue: A Political Analysis

Research Publication 1

by Prof. Donald V. Smiley, York University \$2.00

Freedom of Information and Ministerial Responsibility

Research Publication 2

by Prof. Kenneth Kernaghan, Brock University \$2.00

Public Access to Government Documents: A Comparative Perspective

Research Publication 3

by Prof. Donald C. Rowat, Carleton University \$3.00 (reprint)

Information Access and the Workmen's Compensation Board

Research Publication 4

by Prof. Terence Ison, Queen's University \$5.00 (reprint)

Research and Statistical Uses of Ontario Government Personal Data

Research Publication 5

by Prof. David H. Flaherty, University of Western Ontario \$2.00

Access to Information: Ontario Government Administrative Operations

Research Publication 6

by Hugh R. Hanson et al. \$2.00

Freedom of Information in Local Government in Ontario

Research Publication 7

by Prof. Stanley M. Makuch and Mr. John Jackson \$2.00

cont'd ...

Securities Regulation and Freedom of Information

Research Publication 8

by Prof. Mark Q. Connelly, Osgoode Hall Law School \$2.00

Rule-Making Hearings: A General Statute for Ontario?

Research Publication 9

by Prof. David J. Mullan, Queen's University \$2.00

Freedom of Information and the Administrative Process

Research Publication 10

by Larry M. Fox \$2.00

Government Secrecy, Individual Privacy and the Public's Right to Know:
An Overview of the Ontario Law

Research Publication 11

by Timothy G. Brown \$2.00

Freedom of Information and Individual Privacy: A Selective Bibliography

Research Publication 12

by Laurel Murdoch and Jane Hillard,
with the assistance of Judith Smith \$2.00

Freedom of Information and the Policy-Making Process in Ontario

Research Publication 13

by John Eichmanis \$2.00

Information Access and Crown Corporations

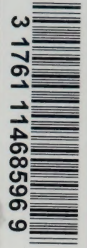
Research Publication 14

by Prof. Isaiah A. Litvak \$2.00

Privacy and Personal Data Protection

Research Publication 15

by Michael Brown, Brenda Billingsley and Rebecca Shamai ... \$5.00



3 1761 11468596 9